University of Alberta

Weil Representations of Finite Symplectic Groups

by

Fernando Szechtman

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements for the degree of Doctor of Philosophy

in

Mathematics.

Department of Mathematical Sciences

Edmonton, Alberta

Spring 1999

National Library of Canada
Acquisitions and Bibliographic Services
395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale du Canada
Acquisitions et services bibliographiques
395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-39598-7

Canada

University of Alberta

Release Form

Name of Author: Fernando Szechtman

Title of Thesis: Weil Representations of Finite Symplectic Groups

Degree: Doctor of Philosophy

Year this Degree Granted: 1999

Permission is hereby granted to the University of Alberta Library to reproduce single copies of this thesis and to lend or sell such copies for private, scholarly or scientific research purposes only.

The author reserves all other publication and other rights in association with the copyright in the thesis, and except as hereinbefore provided neither the thesis nor any substantial portion thereof may be printed or otherwise reproduced in any material form whatever without the author's prior written permission.

(Signed)

Fernando Szechtman
Department of Mathematical Sciences
University of Alberta
Edmonton, Alberta
T6G 2G1
Canada

Date: January 22, 1999

University of Alberta

Faculty of Graduate Studies and Research

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled **Weil Representations of Finite Symplectic Groups** submitted by Fernando Szechtman in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Mathematics.

M. Shirvani

Dr. M. Shirvani (Chair)

Brent Allison

Dr. B. Allison

G. Grondin

Dr. G. Grondin

A. Weiss

Dr. A. Weiss

M.S.

Dr. R. Gow,
University College Dublin, Ireland

Gerald Cliff

Dr. G. Cliff (Supervisor)

Date: January 22, 1999

Dedication

I wish to dedicate this thesis to the five most important people in my life (in the order the appeared in it):

Mabel, mi madre

Natalio, mi padre

Roberto, mi hermano

Cecilia, mi esposa

Malena, mi hija

Abstract

Let R be a finite commutative ring of odd characteristic. Let $\mathrm{Sp}_{2n}(R)$ be the symplectic group associated to a symplectic space of rank $2n$ over R. Weil representations of $\mathrm{Sp}_{2n}(R)$ are carefully defined, explicitly constructed and thoroughly investigated.

Acknowledgement

There is a large number of people that have made my stay in Edmonton a pleasurable one and have helped me in one way or another. Lest I forget an important name (I have been here too long), I collectively thank them all from the bottom of my heart.

Contents

1 Introduction **1**

1.1 Main results 2

1.2 General conventions 6

1.3 To the reader 7

2 Symplectic Groups **8**

2.1 Basic definitions 8

2.2 Generation by symplectic transvections 9

2.3 Generation by elementary matrices 14

2.4 The derived subgroup 18

2.5 The group of symplectic similitudes 20

2.6 Some Sp-orbits 21

2.7 Passage from the local to the general case 24

3 Technical Results **26**

3.1 A generalized Legendre symbol 26

3.2 Quadratic sums 29

3.3 Projective versus Ordinary Representations 41

3.4 Hilbert's Theorem 90 for matrices 44

4 The Schrödinger and Weil Representations **49**

4.1 The existence of the Schrödinger Representation and its consequences . . . 50

4.2 The Weil Representation and its ordinary nature 54
4.3 Reduction to the local case 58
4.4 Uniqueness of the Weil Representation 59

5 Construction of the Weil Representation **60**
5.1 Construction of W on Sp^M 61
5.2 Construction of W on $\mathrm{Sp}_{M,N}$ 62
5.3 Computing P on Sp^N 62
5.4 Computing c on Sp^N 66
5.5 Putting the pieces together 67
5.6 The final product 68
5.7 An alternative approach to compute quadratic sums 69
5.8 Uniqueness of the Weil Representation revisited 71

6 FSp-submodules of X **73**
6.1 The FSp-submodules $X(I)$ of X 73
6.2 $X(I)$ via idempotents of $F(H \rtimes \mathrm{Sp})$ 76
6.3 Explicit decompositions of X 79
6.4 Some character values 81

7 Fundamental properties of the Weil Representations **82**
7.1 The congruence subgroup $\mathrm{Sp}(K)$ acts trivially on $X(I)$ 82
7.2 The FSp-isomorphism $\widehat{JV/IV} \simeq \mathrm{End}_F(X(I))$ 84
7.3 Weil representations associated to different characters 86
7.4 Character fields 89
7.5 Schur indices 90
7.6 The case of a principal ring 92
7.7 The case of a homogeneous ring 96

Examples **98**

Topics for further investigation **100**

Bibliography 102

Index 105

Chapter 1

Introduction

We are interested in the so-called Weil representations of the finite symplectic group $\mathrm{Sp} = \mathrm{Sp}_{2n}(R) = \mathrm{Sp}(R, V, \langle\ ,\ \rangle)$; here R stands for a finite commutative ring with identity and odd characteristic $\mathfrak{c}$, V for a free R-module of rank $2n$ and $\langle\ ,\ \rangle$ for a non-degenerate alternating bilinear form on V. The symplectic group Sp is the subgroup of $\mathrm{GL}(V)$ that preserves $\langle\ ,\ \rangle$.

Weil representations of Sp, when R is the Galois field F_q, have been the subject of intensive research (e.g. [BRW61], [War72], [How73], [Sei75], [Isa73] [Ger77], [Gow89], [Gro90]) and are receiving considerable attention at the moment ([Tie97], [TZ97], [ST97], [Sze98]). Several authors have studied representations of various linear groups over special types of finite commutative rings (e.g. [Tan67], [Lee78], [Hil95]). However, the only literature known to the author on the specific subject under consideration is [CMS].

Weil representations arise as follows. Let $H = H_{2n}(R) = H(R, V, \langle\ ,\ \rangle)$ be the Heisenberg group associated to the symplectic space $(V, \langle\ ,\ \rangle)$; that is $H = \{(r, v) : r \in R, v \in V\}$, with multiplication given by $(r_1, v_1)(r_2, v_2) = (r_1 + r_2 + \langle v_1, v_2\rangle, v_1 + v_2)$. We see at once that $Z(H) = (R, 0) = H'$. Let E be any field whose characteristic does not divide $\mathfrak{c}$ and consider the cyclotomic extension $F = E(\zeta_{\mathfrak{c}})$.

The theory starts off by choosing a non-trivial group homomorphism $\lambda : R^+ \to F^*$. The assumption on E makes this possible. Denote by I_λ the largest ideal contained in $\mathrm{Ker}\,\lambda$ and let $\overline{\lambda}$ be the additive linear character that λ induces on $\overline{R} = R/I_\lambda$. Substituting

R by its epimorphic image $\overline{R}$ and λ by $\overline{\lambda}$, if necessary, we may assume that λ is already primitive, in the sense that $I_\lambda = (0)$. This assumption amounts to saying that each local component R_i of R has a minimum ideal min amongst all its non-zero ideals (Proposition 3.2.3). In other words, (0) must be an irreducible ideal of each R_i (in the terminology of [ZS58], Chapter IV, § 16). These local rings are called irreducible (according to [Lam53], Definition 3).

With these considerations regarding the nature of R and λ behind us, we proceed by extending λ to a maximal abelian subgroup A of H. As it turns out, there are precisely $|R|^n = [H : A] = [A : Z(H)]$ such extensions, and they all can be constructed by means of $\langle\ ,\ \rangle$ and λ itself. In other words, they are all H-conjugate to one another and the inertia group of any of them, say ρ, is A itself. Thus, the induced character $\eta = \mathrm{ind}_A^H \rho$ is an absolutely irreducible character of H over F whose restriction to $Z(H)$ is equal to $|R|^n\lambda$. The characters η and λ are thus fully ramified with respect to $H/Z(H)$, in the sense that η is the unique irreducible character of H lying over λ.

Let Sp act on H by means of ${}^g(r, v) = (r, gv)$. Since Sp acts trivially on $Z(H)$, the irreducible character η^g also lies over λ, and it is therefore equal to η, for each $g \in \mathrm{Sp}$. In other words, η is Sp-invariant. By the Schrödinger representation associated to λ we shall understand any representation $S : H \to \mathrm{GL}(X)$ affording η. Theorem 4.2.6 shows that any such S can be extended to an ordinary (not just projective) representation of $H \rtimes \mathrm{Sp}$ (Theorem 4.2.6), still afforded by X. Its restriction $W = W_\lambda$ to Sp we call the Weil representation of Sp associated to λ.

This thesis is devoted to the study of W.

1.1 Main results

The difficulties in studying W present themselves at the outset, since it is only after a careful study of S that one can convince oneself that W must exist at all. To be concrete we shall assume that $F = \mathbf{Q}(\zeta_\epsilon)$.

After considerable effort Theorem 5.6.1 gives W in matrix form. This requires the

computation of a projective representation $P : \mathrm{Sp} \to \mathrm{GL}(X)$ that intertwines the Sp-conjugates of S and the determination of a correcting factor $c : \mathrm{Sp} \to F^*$ which renders $P(g)$ into an ordinary representation $W(g) = P(g)c(g)$. The precise determination of $c(g)$ involves the computation of certain expressions which are well-known if R is a field but otherwise rather elusive. We are referring to two objects:

The linear character $\mu : R^* \to \{\pm 1\}$, defined by $R^* \ni k \mapsto (-1)^{|\{i \in I \mid ki \in -I\}|} \in \{\pm 1\}$, where I is any subset of $R \setminus \{0\}$ containing precisely one element out of each pair $\{r, -r\}$ of non-zero elements of R and the quadratic sum $\sum(\lambda) = \sum_{r \in R} \lambda(r^2)$. It was Gauss who first determined μ ([Rib72], page 52) and $\sum(\lambda)$ ([Lan70], chapter 4) in the field case. The answer in the general case is given in Section 3.1 for μ and Sections 3.2 and 5.7 for $\sum(\lambda)$. They are unavoidably interwoven.

The Weil representation W is unique unless $\mathrm{Sp}_{2n}(R)$ is imperfect. This can only occur when $n = 1$ and some local component of R has residue field equal to F_3 (Corollary 2.4.4), in which case we carefully select one W to which all our results apply.

The group of symplectic similitudes GSp, which is the subgroup of all $g \in \mathrm{GL}(V)$ that preserve $\langle\ ,\ \rangle$ up to multiplication by a unit $k(g) \in R$, plays an important role in the theory, inasmuch as it allows us to pass from a given W_λ into any other $W_{\lambda'}$. More precisely, any other primitive linear character λ' of R^+ is of the form $\lambda[k]$ (which is λ premultiplied by $k \in R$) and $W_\lambda^g \simeq W_{\lambda[k(g)]}$ for any $g \in \mathrm{GSp}$. Thus, the Weil representations are all GSp-conjugate. Moreover, $W_\lambda \simeq W_{\lambda[k(g)]}$ if and only if $k(g)$ is a square. This is related to the fact that conjugation by $g \in \mathrm{GSp}$ restricts to an inner automorphism of Sp if and only if $k(g)$ is a square. Thus, there are essentially two types of Weil representations, which can be obtained from one another by means of an outer automorphism of Sp coming from GSp (Proposition 5.7.2 and Theorem 7.3.1).

It is possible to assume, and we make this assumption, that R is local ring with residue field F_q and maximal ideal $\mathfrak{m}$ of nilpotency degree $l \geq 1$ (Proposition 4.3.1). Here q is a power of an odd prime p. An important class of examples is obtained by letting $R = \mathcal{O}/\mathfrak{p}^l$, where $\mathcal{O}$ is the ring of integers of an algebraic number field and $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ lying over p. The theory of Weil representations for such rings and more generally, for any

principal local ring R, is very satisfactory. The general case of a general irreducible ring is much more difficult. Nevertheless, quite a lot can still be said about W, as described below.

If Ω denotes the character of W, then the character inner product $[\Omega, \Omega]$ equals the number of Sp-orbits of V. In fact, $\mathrm{End}_F(X)$ and the natural permutation module $\widehat{V}$ arising from V are isomorphic as FSp-modules. An explicit isomorphism is given in Theorem 7.2.1. This recovers the known result ([Isa73] Theorem 4.8, [Ger77] Theorem 4.4) that in the field case the absolutely irreducible components of X are the ± 1-eigenspaces $X^{\pm}$ of the central involution ι of Sp.

Suppose until further notice that R is not a field. This assumption adds entirely new features to the submodule structure of X (which is intimately connected with the ideal structure of R). Indeed, various FSp-submodules of X can be obtained as follows. Fix an an ideal I of R of square (0) and let J be the annihilator of I. Consider next the subgroups $D(I) = (0, IV)$ and $E(J) = (R, JV)$ of H. Then the fixed points $X(I)$ of $D(I)$ in X form an irreducible $F(E(J)/D(I))$-submodule of X of dimension $|J/I|^n$ which is Sp-invariant (Proposition 6.1.2). As such, Theorem 7.1.1 ensures that if $K = (I : J) = \{r \in R \,|\, rJ \subseteq I\}$ is the conductor of J into I then the restriction of the subrepresentation of W afforded by $X(I)$ to the congruence subgroup $\mathrm{Sp}(K) = \{g \in \mathrm{Sp} \,|\, gv \equiv v \bmod KV \text{ for all } v \in V\}$ is trivial.

Let $Y(I)$ be any FSp-invariant complement to $X(I)$ in X and write $Z^{\pm} = Z \cap X^{\pm}$ for any FSp-submodule Z of X. Furthermore, set $Top = Y(\mathrm{min})$ and consider the FSp-decomposition

$$X = Top^{+} \oplus Top^{-} \oplus X(\mathrm{min}). \tag{1.1}$$

Since $\mathfrak{m}^{l-2} \subseteq (\mathrm{min} : \mathfrak{m})$, Theorem 7.1.1 guarantees that $\mathrm{Sp}(\mathfrak{m}^{l-2})$ acts trivially on $X(\mathrm{min})$. Thus (1.1) provides a decomposition of X into those FSp-submodules truly pertaining to Sp and the rest, which in fact constitutes an $\mathrm{FSp}_{2n}(R/\mathfrak{m}^{l-2})$-module. In view of (1.1) the study of X can be carried out according to the following plan:

(1) Describe $Top^{\pm}$ in as much detail as possible.

(2) Study $X(\mathrm{min})$ as a module for the symplectic group $\mathrm{Sp}_{2n}(R/\mathfrak{m}^{l-2})$, associated to the "smaller" ring $R/\mathfrak{m}^{l-2}$.

This is a summary of our progress in these directions:

(1) Theorem 7.2.4 proves that $Top^{\pm}$ are absolutely irreducible FSp-modules of multiplicity one in X and common degree $(|R|^n - |\mathfrak{m}/\mathrm{min}|^n)/2$. Moreover, Proposition 7.2.5 shows that the representations of Sp and PSp respectively afforded by Top^- and Top^+ are faithful.

Write $\mathrm{Sp} \to \mathrm{GL}(\widehat{JV/IV})$ for the F-linear representation arising from the permutation representation $\mathrm{Sp} \to \mathrm{GL}(JV/IV)$. Then Theorem 7.2.1 states that

$$\widehat{JV/IV} \simeq \mathrm{End}_F(X(I)) \tag{1.2}$$

as FSp-modules. If Ω_Z denotes the character of the subrepresentation of W afforded by a given FSp-module Z of X, then (1.2) says that $[\Omega_{X(I)}, \Omega_{X(I)}]$ is equal to the number of Sp-orbits of JV/IV. The absolute irreducibility of $Top^{\pm}$ is consequence of Theorem 7.2.1 applied to $I = (0)$ and $I = \mathrm{min}$.

If R possesses an ideal which is its own annihilator, then the Weil representation of Sp afforded by Top and $Top^{\pm}$ are monomial (Theorem 7.7.1).

The character field of $Top^{\pm}$ or, for that matter, any $Y(I)^{\pm}$ is equal to $\mathbf{Q}\left(\sqrt{(\frac{-1}{q})q}\right)$ (Theorem 7.4.1).

Top^+ can be always be realized over its character field (Theorem 7.5.1).

Top^- can be realized over its character field if and only if $\mathbf{Q}\left(\sqrt{(\frac{-1}{q})q}\right)$ is not a real field; that is, $q \equiv 3 \mod 4$ (Theorem 7.5.1). Thus, if $q \equiv 1 \mod 4$ then the Schur index $m_{\mathbf{Q}}(\Omega_{Top^-})$ is equal to two due to the Brauer-Speiser Theorem.

(2) If R is principal, say $\mathfrak{m} = (\pi)$, then Theorem 7.6.2 shows that the representation of $\mathrm{Sp}_{2n}(R/\mathfrak{m}^{l-2})$ afforded by $X(\mathrm{min})$ is equal to the Weil representation associated to the primitive linear character of $R/\mathfrak{m}^{l-2}$ defined by $r + \pi^{l-2}R \mapsto \lambda(r\pi^2)$. This results constitutes, in effect, a truly recursive procedure to study the irreducible components of W. There are $l+1$ of them, all inequivalent to one another.

The case of a general irreducible ring R is more difficult. We are currently working on this problem.

The field case is of particular interest. In this case, not only do we know when $X^{\pm}$ can be realized over $\mathbf{Q}(\Omega_{X^{\pm}})$ [Gow89], but we can actually perform the realization explicitly, whenever possible. In other words we can write down an explicit family of matrices A, each of which conjugates the matrix Weil representations over F associated to $X^{\pm}$ (as given in Theorem 5.6.1) into matrix representations with coefficients in the character fields $\mathbf{Q}(\Omega_{X^{\pm}})$, provided $m_{\mathbf{Q}}(\Omega_{X^{\pm}}) = 1$. This result can be found in [Sze98].

Furthermore, [Sze98] constructs Weil representations of GSp, realizes them over their character fields and determines the Sp and GSp-invariant bilinear forms that are uniquely associated -up to scaling- to their Weil components, whenever self-contragredient. These results easily extend to the general case of an irreducible ring R.

Finally, we can embed the finite unitary group $\mathrm{U}_n(q)$ canonically into $\mathrm{Sp}_{2n}(q)$ and study the restriction of W to $\mathrm{U}_n(q)$ and various of its subgroups, most notably $\mathrm{SU}_n(q)$. This material can be found in [Sze], in the case when n is even.

1.2 General conventions

We shall assume throughout that R is a finite commutative ring with 1 and odd characteristic $\mathfrak{c}$; that is, 2 is invertible in $\mathbf{Z}/\mathfrak{c}\mathbf{Z} \subseteq R$. Further assumptions on R will be specifically stated in each chapter or section if needed. We shall write $R = R_1 \times ... \times R_t$, the decomposition of R into local rings ([AM69], chapter 8). Given an integer $s \geq 1$, denote by ζ_s a primitive s-th root of unity. Let F be the cyclotomic field $F = \mathbf{Q}(\zeta_{\mathfrak{c}})$.

Should R be a local ring itself, its maximal ideal will be denoted by $\mathfrak{m}$ and its residue field $R/\mathfrak{m}$ by F_q, where q is a power of an odd prime p. Since R is finite $\mathfrak{m}$ is nilpotent, say with nilpotency degree $l \geq 1$. We shall also write $|R| = q^{d_R}$ and $\mathfrak{c} = p^e$.

Composition of functions proceeds from right to left. Accordingly, left actions are associated to homomorphisms and right actions to anti-homomorphism. If G is a group and $g, h \in G$, then ${}^g h = ghg^{-1}$. Suppose that E_1, E_2 are sets being acted upon from the

left by G. Then G acts on the right on the set of functions f from E_1 into a fixed set Δ

$$(f^g)(x) = f({}^g x)$$

and on the left on the set of functions $f : \Delta \to E_2$, by means of

$$({}^g f)(x) = {}^g(f(x)).$$

We shall usually take f to be W or Ω; then G will act on the right disguised as GSp and on left as $\mathrm{Gal}(F/\mathbf{Q})$.

This thesis contains many more variables (letters, symbols) than any one can retain at any given moment. To facilitate the reading, we have included a list of symbols at the end of the text, where one can find the first appearance of every letter that has a global meaning. We allow locally defined variables to have different meanings in different sections. We strive to adhere to standard terminology and notation.

1.3 To the reader

To get an overall idea of this work read the Introduction. Chapters 2 and 3 contain necessary but auxiliary material; these results can be read as they become necessary elsewhere in the text. Chapter 4 lays the foundations of the theory of Weil representations; it must be read.

If there is one topic whose elaboration required far more time than any other in this thesis it is the construction of W given in Chapter 5. With it, the author had the opportunity to see representation theory in action for the first time. Starting the process with $\mathrm{SL}_2(p)$, and passing through $\mathrm{SL}_2(q)$, $\mathrm{Sp}_{2n}(q)$ and $\mathrm{Sp}_{2n}(R)$ for a principal ring R, a complete solution was finally attained for a general irreducible ring R. Highly recommended, but not logically necessary on a first reading.

Chapter 6 develops the language to be used later in Chapter 7. Read up to Proposition 6.1.2 inclusive, and come to it afterwards as it becomes necessary. The last chapter contains mostly theorems, the ones described in the Introduction. It must be read.

Chapter 2

Symplectic Groups

This chapter is included for the sake of completeness. It contains no new results. The presentation is inspired by [Die48] with help from [Jac85]. Further references are [O'M78] for the field case, [Kli63] for the local case and [HO89] for utmost generality.

2.1 Basic definitions

Let V be a free module of rank $2n$ over R. An alternating bilinear form on V is a map $\langle\ ,\ \rangle : V \times V \to R$ satisfying

$$\langle rx + sy, z\rangle = r\langle x, z\rangle + s\langle y, z\rangle,$$

$$\langle x, ry + sz\rangle = r\langle x, y\rangle + s\langle x, z\rangle,$$

$$\langle x, x\rangle = 0 \tag{2.1}$$

for all $x, y, z \in V$ and $r, s \in R$. Since 2 is invertible in R (2.1) is equivalent to

$$\langle x, y\rangle = -\langle y, x\rangle$$

for all $x, y \in V$.

We shall not be concerned here with just any alternating form (e.g. the zero form), but only with those $\langle\ ,\ \rangle$ whose associated map from V into its dual space V^*

$$V \ni v \mapsto \langle v, -\rangle \in V^* \tag{2.2}$$

is an monomorphism. Since V^* is also free of rank $2n$ and R is finite

$$|V^*| = |V| = |R|^{2n},$$

whence (2.2) is an isomorphism. We fix one such $\langle\ ,\ \rangle$ and refer to $(V, \langle\ ,\ \rangle)$ as a symplectic space of rank $2n$ over R.

Let Sp denote the symplectic group associated to the symplectic space $(V, \langle\ ,\ \rangle)$; that is

$$\mathrm{Sp} = \mathrm{Sp}(R, V, \langle\ ,\ \rangle) = \mathrm{Sp}_{2n}(R) = \{g \in \mathrm{GL}(V) : \langle gv, gv' \rangle = \langle v, v' \rangle \text{ for all } v, v' \in V\}.$$

The elements of Sp are called symplectic transformations. For instance, if $r \in R$ and $x \in V$ then the map $\rho_{r,x}$ defined by

$$v \mapsto v + r\langle x, v \rangle x$$

is a symplectic transformation. Observe the relations

$$g\rho_{r,x}g^{-1} = \rho_{r,gx}, \tag{2.3}$$

$$\rho_{r,sx} = \rho_{rs^2,x}, \tag{2.4}$$

$$\rho_{r+s,x} = \rho_{r,x}\rho_{s,x}, \tag{2.5}$$

valid for all $g \in \mathrm{Sp}$, $r, s \in R$ and $x \in V$.

We proceed to describe symplectic groups and spaces in as much detail as is necessary later in the text. We treat the case when R is local and indicate in Section 2.7 how to deal with the general case.

2.2 Generation by symplectic transvections

We shall assume here that R is local. We summarize below the basic properties of local rings to be used in the sequel.

2.2.1 Lemma (a) The cardinality of every ideal of R is a power of q.

(b) Every element of the multiplicative group $1+\mathfrak{m}$ is a square.

(c) $k \in R^*$ is a square if and only if $k+\mathfrak{m} \in F_q$ is a square.

(d) $k^2 = 1$ if and only if $k = \pm 1$. Thus $R^*/(R^*)^2 \simeq C_2$, whence the only group homomorphisms from R^* into $\{\pm 1\}$ are the trivial homomorphism and the Legendre symbol

$$k \mapsto (\frac{k}{R}) = \begin{cases} 1 & \text{if } k \text{ is a square} \\ -1 & \text{otherwise} \end{cases}.$$

(e) $R^* = (1+\mathfrak{m}) \times U$, where $U \simeq F_q^*$ is the unique subgroup of R^* of order $|R^*/1+\mathfrak{m}|$.

(f) Every element of $(\mathbf{Z}/p^e\mathbf{Z})^* \subseteq R^*$ is a square if and only if q is a square.

Proof: (a) Form the F_q-spaces $\mathfrak{m}^i I/\mathfrak{m}^{i+1} I$ and count.

(b) $|1+\mathfrak{m}| = |\mathfrak{m}|$ is a power of q and hence odd.

(c) If $k = r^2 + s$ for some $s \in \mathfrak{m}$ and $r \in R^*$ then $k = r^2(1+r^{-2}s) = r^2t^2 = (rt)^2$ for the unique $t \in 1+\mathfrak{m}$ satisfying $t^2 = 1+r^{-2}s$.

(d) If $(k-1)(k+1) = 0$ then $k-1$ or $k+1 \in \mathfrak{m}$, but not both since $2 \notin \mathfrak{m}$; thus precisely one of them is a unit, whence $k = 1$ or else $k = -1$.

(e) The order $\frac{|R|-|\mathfrak{m}|}{|\mathfrak{m}|} = \frac{|R|}{|\mathfrak{m}|} - 1$ of $R^*/1+\mathfrak{m}$ is coprime to the order $|\mathfrak{m}|$ of $1+\mathfrak{m}$. Thus the exact sequence $1 \to 1+\mathfrak{m} \to R^* \to F_q^* \to 1$ splits.

(f) The image of $\mathbf{Z} \ni z \mapsto z.1_R \in R$ lives in the prime field F_p of F_q modulo $\mathfrak{m}$. Now apply (c). □

A symplectic basis is a basis

$$\{u_1, u_2, \ldots, u_n, v_1, v_2, \ldots, v_n\} \tag{2.6}$$

of V such that

$$\langle u_i, u_j \rangle = \langle v_i, v_j \rangle = 0, \quad \langle u_i, v_j \rangle = -\langle v_j, u_i \rangle = \delta_{ij}.$$

By a primitive vector we shall understand a vector belonging to some basis of V. The set of all such vectors will be denoted by $\mathcal{P}$. Thus $\mathcal{P} = V \setminus \mathfrak{m}V$. A pair of vectors (u, v) will be called hyperbolic if $\langle u, v \rangle = 1$. The set of all such pairs will be denoted by HP.

Given a subset L of V let

$$L^{\perp} = \{v \in V \mid \langle v, x\rangle = 0 \text{ for all } x \in L\}$$

and

$$L^{0} = \{v^{*} \in V^{*} \mid v^{*}(x) = 0 \text{ for all } x \in L\}.$$

Thus $L^{\perp}$ is the preimage of L^{0} under (2.2).

2.2.2 Lemma The following conditions are equivalent:

(a) V has a symplectic basis.

(b) The map (2.2) is an isomorphism.

(c) Every element $w \in \mathcal{P}$ belongs to a symplectic basis.

Proof: (a)⇒(b) and (c)⇒(a) are clear. (b)⇒(c) Given $w \in \mathcal{P}$, let $\{w, e_2, ..., e_{2n}\}$ be a basis of V. Choose an element $z = r_1 w + r_2 e_2 + ... + r_{2n} e_{2n} \in V$ satisfying $\langle w, z\rangle = 1$. Some coefficient r_i, with $i \geq 2$ must be a unit. Relabeling if necessary we can assume that r_{n+1} is a unit, whence $\{w, e_2, e_3, ...e_n, z, e_{n+2}, ..., e_{2n}\}$ is a basis of V.

Write $f_i = e_i - \langle e_i, z\rangle w + \langle e_i, w\rangle z$, $i \neq 1, n+1$, $U_0 = Rw \oplus Rz$, $U = \oplus_{i \neq 1, n+1} Rf_i$ and $\langle\ ,\ \rangle_U = \langle\ ,\ \rangle|_{U \times U}$. Then $V = U_0 \oplus U$, $U_0^{\perp} = U$ and $(U, \langle\ ,\ \rangle_U)$ is a symplectic space of rank $2(n-1)$. By recurrence $(U, \langle\ ,\ \rangle_U)$ has a symplectic basis, which can be adjoined to $\{w, ..., z, ...\}$ to yield a symplectic basis of V. □

We shall fix the basis (2.6) throughout. A simple but useful observation is that $g \in \mathrm{GL}(V)$ belongs to Sp if and only if g maps symplectic bases into symplectic bases.

As a result of Lemma 2.2.2 we obtain

2.2.3 Corollary $\mathcal{P} = V \setminus \mathfrak{m}V$ is an Sp-orbit.

Given an ideal I of R, denote by $\mathrm{Sp}(I) = \mathrm{Sp}_{2n}(I)$ the congruence subgroup associated to I, that is, $\mathrm{Sp}(I) = \{g \in \mathrm{Sp} \mid gv \equiv v \mod IV\}$. A symplectic transformation g is called a symplectic transvection if $g = \rho_{r,x}$ for some primitive vector $x \in V$ and some $r \in R$. Alternatively, if the matrix of g relative to some symplectic basis is elementary. According to this definition, $\rho_{r,x} \in \mathrm{Sp}(I)$ if and only if $r \in I$. Denote temporarily by $T_{2n}(I)$ the subgroup of $\mathrm{Sp}_{2n}(R)$ generated by $(\rho_{r,x})_{r \in I, x \in \mathcal{P}}$.

2.2.4 Lemma Suppose that $n = 1$ and let I be an ideal of R. Then $\mathrm{Sp}(I)$ is generated by symplectic transvections.

Proof: In matrix form, we need to prove that

$$\mathrm{SL}_2(I) = \{A \in \mathrm{SL}_2(R) \mid A - 1 \in M_2(I)\}$$

is generated by

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \quad r, s \in I \tag{2.7}$$

and their conjugates.

Suppose first that $I \neq R$. Given $\begin{pmatrix} 1+r & r_2 \\ r_3 & 1+r_4 \end{pmatrix} \in \mathrm{SL}_2(I)$, denote the inverse of $1+r$ by s. Then

$$\begin{aligned} \begin{pmatrix} 1+r & 0 \\ 0 & s \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -r_3 s & 1 \end{pmatrix} \begin{pmatrix} 1+r & r_2 \\ r_3 & 1+r_4 \end{pmatrix} \begin{pmatrix} 1 & -r_2 s \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ rs & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -rs \\ 0 & 1 \end{pmatrix}, \end{aligned}$$

whence $\mathrm{SL}_2(I)$ is indeed generated by (2.7) and their conjugates.

If $I = R$ the above reasoning remains valid, provided $1+r$ is invertible. If this is not the case, then r_3 is certainly invertible, whence the $(1,1)$-entry of $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1+r & r_2 \\ r_3 & 1+r_4 \end{pmatrix}$ is now invertible and the above reasoning applies. □

We have proven, incidentally, that

2.2.5 Proposition $\mathrm{SL}_2(R)$ is generated by

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \quad r, s \in R.$$

The corresponding result for $\mathrm{SL}_2(I)$ is false.

2.2.6 Proposition Let I be an ideal of R. Then $\mathrm{Sp}_{2n}(I)$ is generated by symplectic transvections.

Proof: By induction on n. The base case $n = 1$ was proved in Lemma 2.2.4. Suppose that $n > 1$ and the result is true for all $1 \leq m < n$. Let $\mathrm{T}_{2n}(I)$ act on $\mathcal{P}$ and HP, and denote the relation of being in the same $\mathrm{T}_{2n}(I)$-orbit by $\sim$.

Claim. Every $\mathrm{Sp}_{2n}(I)$-orbit of HP is a $\mathrm{T}_{2n}(I)$-orbit.

Suppose the Claim is true. Given $g \in \mathrm{Sp}_{2n}(I)$ and (w, z) in HP, choose $g_0 \in T_{2n}(I)$ such that $g \cdot (w, z) = g_0 \cdot (w, z)$. Write $U_0 = Rw \oplus Rz$, $U = U_0^{\perp}$ and $V = U_0 \oplus U$ as in the proof of Lemma 2.2.2. The inductive hypothesis applies, yielding $gg_0^{-1} \in T_{2n}(I)$, whence $g \in T_{2n}(I)$.

We prove the Claim when $I \neq R$. The case $I = R$ is similar and will be omitted. Fix any hyperbolic pair (w, z). To see the Claim is suffices to prove that

1. $w \sim w + v$ for all $v \in IV$.

2. $(w, z) \sim (w, z + v)$ for all $v \in IV$ such that $(w, z + v) \in \mathrm{HP}$.

Observe that 1 and 2 can be obtained by repeated application of

1'. $w \sim w + rv$ for all $r \in I$ and $v \in \mathcal{P}$.

2'. $(w, z) \sim (w, z + rv)$ for all $r \in I$ and $v \in \mathcal{P}$ such that $(w, rv) = 0$.

We proceed to the proof of 1' and 2'. Let $r \in I$ and $v \in \mathcal{P}$. Suppose that $\langle v, w \rangle$ is a unit in R. Then $\rho_{r\langle v,w\rangle^{-1},v} w = w + rv$. If $\langle v, w \rangle$ is not a unit, then $\langle z, w \rangle$ and $\langle v - z, w + rz \rangle$ are certainly units, whence $w \sim w + rz \sim w + rz + r(v - z) = w + rv$. This establishes 1'. To see 2' observe that if $\langle v, z \rangle$ is a unit, then $\rho_{r\langle v,z\rangle^{-1},v}(w, z) = (w, z + rv)$. If $\langle v, z \rangle$ is not a unit, then $\langle w + v, z \rangle$ and $\langle -w, z + r(w + v) \rangle$ are certainly units, whence $(w, z) \sim (w, z + r(w + v)) \sim (w, z + r(w + v) - rw) = (w, z + rv)$, as desired. □

2.2.7 Corollary Given an ideal I of R and a primitive vector $x \in V$, the normal closure of $(\rho_{r,x})_{r \in I}$ is equal to $\mathrm{Sp}(I)$.

Proof: This is consequence of Proposition 2.2.6, Corollary 2.2.3 and (2.3). □

2.2.8 Theorem Suppose that $q > 3$. Then the only normal subgroups of Sp are its center $\{1, \iota\}$, the congruence subgroups $\mathrm{Sp}(I)$ and the subgroups $\{1, \iota\}\mathrm{Sp}(I)$, where I runs through all ideals of I.

Proof: See [Kli63]. □

2.3 Generation by elementary matrices

Assume here that R is local.

Set $M = Ru_1 \oplus ... \oplus Ru_n$ and $N = Rv_1 \oplus ... \oplus Rv_n$. Denote by Sp_M the subgroup of Sp preserving M (and similarly for other submodules of V), by Sp^M the one fixing every point of M and by $\mathrm{Sp}_{M,N}$ the one preserving both M and N. Let $S_n(R)$ be the abelian (additive) group of all $n \times n$ symmetric matrix with coefficients in R. Then relative to the symplectic basis (2.6)

$$S_n(R) \ni S \leftrightarrow B(S) = \left(\begin{array}{c|c} 1 & S \\ \hline 0 & 1 \end{array}\right) \in \mathrm{Sp}^M,$$

$$S_n(R) \ni S \leftrightarrow C(S) = \left(\begin{array}{c|c} 1 & 0 \\ \hline S & 1 \end{array}\right) \in \mathrm{Sp}^N,$$

and

$$\mathrm{GL}_n(R) \ni A \leftrightarrow D(A) = \left(\begin{array}{c|c} A & 0 \\ \hline 0 & (A^{-1})^t \end{array}\right) \in \mathrm{Sp}_{M,N} \tag{2.8}$$

are group isomorphisms. The natural actions

$$^A S = ASA^t, \quad ^A S = (A^{-1})^t S A^{-1}$$

of $\mathrm{GL}_n(R)$ on $S_n(R)$ translate into

$$^{D(A)}B(S) = B(ASA^t), \quad ^{D(A)}C(S) = C((A^{-1})^t S A^{-1}), \tag{2.9}$$

whence

$$\mathrm{Sp}_M = \mathrm{Sp}^M \rtimes \mathrm{Sp}_{M,N} \simeq S_n(R) \rtimes \mathrm{GL}_n(R)$$

and

$$\mathrm{Sp}_M = \mathrm{Sp}^N \rtimes \mathrm{Sp}_{M,N} \simeq S_n(R) \rtimes \mathrm{GL}_n(R).$$

Observe that M and N are totally isotropic, in the sense that $\langle\ ,\ \rangle$ vanishes on them, and they are maximal relative to this property. Denote by $\mathcal{M}$ the collection of all maximal totally isotropic submodules of V. As opposed to the field case, not all members of $\mathcal{M}$

are in the same Sp-orbit. In fact, they need not be even isomorphic as groups. This phenomenon is due to the presence of members of $\mathcal{M}$ constructed as follows.

Let (I, J) be any pair of ideals of R and consider the submodule $L_{I,J} = IN \oplus JM$ of V. Then $L_{I,J}$ is totally isotropic if and only if $IJ = (0)$ and $L_{I,J} \in \mathcal{M}$ if and only if the annihilator $\mathrm{Ann}(I)$ of I is equal to J and vice versa. In fact, we have the following result:

2.3.1 Lemma Let I, J be ideals of R. Denote by I' and J' the annihilators of I and J, respectively. Then

$$L_{I,J}^{\perp} = L_{J',I'}.$$

Proof: This follows from the very definitions of the objects involved. □

One subset of $\mathcal{M}$ stands out, namely the one comprising only free submodules of V. Denote by $\mathcal{F}$ the set of all free submodules of V. We record a few properties of members of these classes.

2.3.2 Lemma Let $L \in \mathcal{M}$. Then for any $g \in \mathrm{Sp}^L$ we have

(a) $gx - x \in L$ for all $x \in V$.

(b) $\langle x, gy - y \rangle = \langle y, gx - x \rangle$ for all $x, y \in V$.

Proof: The argument given in [Die48], pages 7-8, goes through verbatim. □

2.3.3 Lemma A submodule L of V is free if and only if it is complemented.

Proof: It is a standard result that every projective module over a local ring is free. Given a basis $\{e_1, ..., e_{2n}\}$ of V and $\{f_1, ..., f_r\}$ of $L \in \mathcal{F}$, write $f_1 = \sum_{1 \le i \le 2n} r_i e_i$. One of the r_i is a unit, for otherwise $\mathfrak{m}^{l-1} f_1 = 0$. There exists thus a basis $\{f_1, e_2', ..., e_{2n}'\}$ of V. Suppose we have found a basis $\{f_1, ..., f_t, e_{t+1}'', ..., e_{2n}''\}$ of V and write $f_{t+1} = \sum_{1 \le i \le t} s_i f_i + \sum_{t+1 \le i \le 2n} \gamma_i e_i''$. If no γ_i is a unit then $\mathfrak{m}^{l-1} f_{t+1} \subseteq \mathfrak{m}^{l-1} f_1 + ... + \mathfrak{m}^{l-1} f_t$, contradicting the linear independence of the f_i. The above process can thus be continued, yielding a basis $\{f_1, ..., f_r, e_{r+1}''', ..., e_{2n}'''\}$ of V. □

2.3.4 Lemma (a) Every $L \in \mathcal{M} \cap \mathcal{F}$ has rank n.

(b) Given $L \in \mathcal{M} \cap \mathcal{F}$ there exists a hyperbolic pair (w, z) such that $w \in L$, and any such pair belongs to some symplectic basis of V that contains a basis of L.

(c) Sp acts transitively on $\mathcal{M} \cap \mathcal{F}$ and also on the set of all pairs (L_0, L_1) that belong to $\mathcal{M} \cap \mathcal{F}$ and satisfy $L_0 \oplus L_1 = V$.

Proof:

(a) If $L \in \mathcal{M} \cap \mathcal{F}$ has rank r then $L = L^\perp$ is the preimage of L^0 under the isomorphism (2.2), and has therefore rank $2n - r$. The invariance of rank forces $r = n$.

(b) Let $\{e_1, ..., e_n\}$ be a basis of L. Extend it to a basis $\{e_1, ..., e_n, e_{n+1}, ..., e_{2n}\}$ of V as in Lemma 2.3.3 and set $w = e_1$. Then Lemma 2.2.2 ensures the existence of a hyperbolic pair (w, z). Define f_i, $i \neq 1, n+1$, U_0, U and $\langle\ ,\ \rangle_U$ as in the proof of Lemma 2.2.2. Then the basis $\{f_2, ..., f_n, f_{n+2}, ..., f_{2n}\}$ of U contains the basis $\{f_2, ..., f_n\}$ of $U \cap L$. By recurrence, there exists a symplectic basis of U that contains a basis of $U \cap L$. Adjoining (w, z) to this basis we obtain the desired result.

(c) The first assertion follows from (b); for the second, start with bases $\{e_1, ..., e_n\}$ of L_0 and $\{e_{n+1}, ..., e_{2n}\}$ of L_1 and proceed as in the proof of (b), mutatis mutandis. □

2.3.5 Proposition $\langle \mathrm{Sp}_M, \mathrm{Sp}_N \rangle$ acts transitively on $\mathcal{P}$.

Proof: Let $z \in \mathcal{P}$. Then either $\langle M, z \rangle = R$ or $\langle N, z \rangle = R$; say $\langle w, z \rangle = 1$ for some $w \in M$. Then Lemma 2.3.4 ensures the existence of $g \in \mathrm{Sp}_M$ satisfying $gv_1 = z$. □

2.3.6 Proposition $\langle \mathrm{Sp}_M, \mathrm{Sp}_N \rangle = \mathrm{Sp}$.

Proof: Sp_M contains all transvections ρ_{r,u_1}, $r \in R$. Given a transvection $\rho_{r,x}$, such that $x \in \mathcal{P}$, Corollary 2.3.5 ensures the existence of $g \in \langle \mathrm{Sp}_M, \mathrm{Sp}_N \rangle$ such that $gu_1 = x$. Hence $\rho_{r,x} = g\rho_{r,u_1}g^{-1} \in \langle \mathrm{Sp}_M, \mathrm{Sp}_N \rangle$. The result now follows from Proposition 2.2.6. □

The generating set $\mathrm{Sp}^M \cup \mathrm{Sp}_{M,N} \cup \mathrm{Sp}^N$ is still too big to be any practical use. A first simplification can be obtained as follows. Let

$$g_{M,N} = \left(\begin{array}{c|c} 0 & -1 \\ \hline 1 & 0 \end{array}\right).$$

Then

$$g_{M,N}^2 = \iota = \left(\begin{array}{c|c} -1 & 0 \\ \hline 0 & -1 \end{array}\right),$$

$$g_{M,N} B(S) = C(-S) \tag{2.10}$$

and

$$g_{M,N} D(A) = D((A^{-1})^t). \tag{2.11}$$

We deduce that

$$g_{M,N} Sp_M = \mathrm{Sp}_N,$$

whence

2.3.7 Corollary Sp is generated by $\mathrm{Sp}^M \cup \mathrm{Sp}_{M,N} \cup \{g_{M,N}\}$.

A slight variation of Corollary 2.3.7 can be obtained as follows. Given $r \in R$ define the elements $g^M(r)$ and $g^N(r)$, respectively belonging to Sp^M and Sp^N, by

$$g^M(r) = \left(\begin{array}{c|c} 1 & r \\ \hline 0 & 1 \end{array}\right), \quad g^N(r) = \left(\begin{array}{c|c} 1 & 0 \\ \hline r & 1 \end{array}\right).$$

Then

$$g_{M,N} = g^M(-1) g^N(1) g^M(-1), \tag{2.12}$$

whence

2.3.8 Corollary Sp is generated by $\mathrm{Sp}^M \cup \mathrm{Sp}_{M,N} \cup \{g^N(1)\}$.

It is on the generating sets given in Corollaries 2.3.7 and 2.3.8 that the Weil representation will be defined. The next, and last, generating set can be used in conjunction with Theorem 5.6.1 to produce concrete examples of Weil representations.

Denote by E^{ij} the $n \times n$ matrix having a 1 in the (i,j)-entry and 0 everywhere else. Then

$$\rho_{r,u_i} = B(rE^{ii}), \quad 1 \le i \le n \tag{2.13}$$

and

$$\rho_{r,u_i+u_j} - \rho_{r,u_i} - \rho_{r,u_j} = B(r(E^{ij} + E^{ji})), \quad 1 \leq i \neq j \leq n,$$

whence

2.3.9 Lemma Sp^M is generated by $B(rE^{ii})$ and $B(r(E^{ij}+E^{ji}))$, when r runs through R and $1 \leq i \neq j \leq n$.

Observe also that

2.3.10 Lemma (a) $\mathrm{SL}_d(R)$ is generated by elementary matrices.

(b) $\mathrm{GL}_d(R)' = \mathrm{SL}_d(R)$.

(c) $\mathrm{GL}_d(R) = \mathrm{SL}_d(R) \rtimes \{\mathrm{diag}(k, 1, ..., 1) \mid k \in R^*\}$.

Proof: Reason as in the field case, mutatis mutandis. □

We can finally state

2.3.11 Proposition Sp is generated by

$$B(rE^{ii})_{1 \leq i \leq n},\ B(r(E^{ij} + E^{ji}))_{1 \leq i \neq j \leq n},\ D(1 + rE^{ij})_{1 \leq i < j \leq n},\ g_{M,N}$$

when r runs through R.

Proof: Denote temporarily by G the subgroup generated by the alluded matrices. In view of Lemma 2.3.9 and (2.10), G contains Sp^M and Sp^N. On the other hand, due to Lemma 2.3.10(a) and (2.11) G contains $\{D(A) \mid \det A = 1\}$. However, in light of (2.10) and Proposition 2.2.5 $B(rE^{11})$ and $g_{M,N}$ suffice to generate $\{D(\mathrm{diag}(k, 1, ..., 1)) \mid k \in R^*\}$. Thus Lemma 2.3.10(c) ensures that G contains also $\mathrm{Sp}_{M,N}$, and must therefore be equal to Sp. □

2.4 The derived subgroup

Assume here that R is local.

2.4.1 Proposition $\mathrm{Sp}_{2n}(R)$ is perfect if $q > 3$.

Proof: In view Proposition 2.2.6 it suffices to show that every $\rho_{r,x}$ is in Sp' when $x \in \mathcal{P}$. Since $R/\mathfrak{m}$ has more than three elements there exists a $k \in R^*$ such that $k^2 - 1$ is also a unit. Set $s = (k^2-1)^{-1}r$. Since x and kx are primitive Corollary 2.2.3 ensures the existence of a $g \in \mathrm{Sp}$ satisfying $gx = kx$. Now (2.3) and (2.4) yield $g\rho_{s,x}g^{-1} = \rho_{sk^2,x}$, whence (2.5) gives

$$[g, \rho_{s,x}] = \rho_{(k^2-1)s,x} = \rho_{r,x},$$

as required. □

2.4.2 Proposition $\mathrm{Sp}_{2n}(R)$ is perfect if $n \geq 2$.

Proof: There is no loss of generality in assuming that $n = 2$. Given $r \in R$, let $S_r = \left(\begin{array}{c|c} r & 0 \\ \hline 0 & 0 \end{array}\right) \in S_2(R)$. In view of (2.9), (2.13) and Proposition 2.2.6 it suffices to find $A \in \mathrm{GL}_2(R)$ and $S \in S_2(R)$ such that $A^tSA - S = S_r$.

For this purpose, let $S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and think of S as the matrix of a bilinear form B on a free R-module with basis $\{w, z\}$. Then the matrix of B relative to $\{w + tz, z\}$ will be $\begin{pmatrix} 2t & 1 \\ 1 & 0 \end{pmatrix}$; that is, if $A = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$ is the matrix associated to the change of basis, then $A^tSA = \begin{pmatrix} 2t & 1 \\ 1 & 0 \end{pmatrix}$. Since 2 is invertible in R we can choose t so that $2t = r$, whence $A^tSA - S = S_0$, as required. □

2.4.3 Proposition If $n = 1$ and $q = 3$ then $\mathrm{Sp}(\mathfrak{m}) \subseteq \mathrm{Sp}'$ and $[\mathrm{Sp} : \mathrm{Sp}'] = 3$.

Proof: Denote by $^-$ the epimorphism $\mathrm{Sp} \to \mathrm{Sp}_{\mathfrak{m}} = \mathrm{Sp}_2(3)$ and by D and $\overline{D}$ the derived groups of Sp and $\overline{\mathrm{Sp}}$, respectively. Since $[\overline{\mathrm{Sp}} : \overline{D}] = 3$ we have $[\mathrm{Sp} : D\mathrm{Sp}(\mathfrak{m})] = 3$. It remains to show that $\mathrm{Sp}(\mathfrak{m}) \subseteq D$.

Given $r \in \mathfrak{m}$, choose $k \in 1+\mathfrak{m}$ so that $k^2 = 1+r$; that is, $k^2 - 1 = r$. Set $g_0 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $g_1 = \begin{pmatrix} k^{-1} & 0 \\ 0 & k \end{pmatrix}$. Thus any $\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} = [g_1, g_0]$ belongs to D. The result now follows from Corollary 2.2.7. □

2.4.4 Corollary Sp is imperfect if and only if $n = 1$ and $q = 3$, in which case there are precisely three group homomorphisms $\tau_i : \mathrm{Sp} \to F^*$, given by $\tau_i(\rho_{1,u_1}) = \zeta_3^i$, $\quad 0 \leq i < 3$.

Proof: The first assertion is consequence of Propositions 2.4.1, 2.4.2 and 2.4.3; for the second inflate the corresponding homomorphisms from $\mathrm{Sp}_2(3)$. □

2.5 The group of symplectic similitudes

Denote by GSp the group of symplectic similitudes

$$\mathrm{GSp} = \{g \in \mathrm{GL}(V) : \exists\, k(g) \in R^* \text{ such that } \langle gv, gv' \rangle = k(g)\langle v, v' \rangle \text{ for all } v, v' \in V\}.$$

We record a few properties of GSp to be used in the sequel. The scalar $k(g)$ is uniquely attached to $g \in \mathrm{GSp}$. Moreover, given g_1, $g_2 \in \mathrm{GSp}$ we have

$$k(g_1 g_2) = k(g_1)k(g_2). \tag{2.14}$$

Given $k \in R^*$ define the elements $g_k \in \mathrm{Sp}$ and $B_k \in \mathrm{GSp}$ by

$$g_k = \left(\begin{array}{c|c} k & 0 \\ \hline 0 & k^{-1} \end{array}\right), \quad B_k = \left(\begin{array}{c|c} k & 0 \\ \hline 0 & 1 \end{array}\right).$$

We easily see that, abusing our notation,

$$k(B_k) = k \tag{2.15}$$

and

$$\mathrm{GSp} = \mathrm{Sp} \rtimes \langle (B_k)_{k \in R^*} \rangle. \tag{2.16}$$

Observe also the important relations

$$B_{k^2} \cdot k^{-1} \cdot 1_V = g_k \tag{2.17}$$

and

$${}^{B_k} g_{M,N} = g_k g_{M,N}. \tag{2.18}$$

Note also that

$$^{B_k}g \in \mathrm{Sp}_{M,N}, \tag{2.19}$$

$$\det\,(^{B_k}g)|_N = \det\, g|_N \tag{2.20}$$

for all $g \in \mathrm{Sp}_{M,N}$, and

$$^{B_k}g^N(r) = g^N(k^{-1}r) \tag{2.21}$$

for all $r \in R$.

2.6 Some Sp-orbits

Assume that R is local.

If $G \to Sym(\Delta)$ is a permutation representation of a finite group G and $x \in \Delta$, we shall denote by O_x the G-orbit of Δ containing x, by $O(\Delta)$ the set of G-orbits of Δ and by $o(\Delta)$ the cardinality of $O(\Delta)$. The relation of being in the same G-orbit will be denoted by $\sim$. We record a few facts pertaining to the set-up $G = \mathrm{Sp}$ and $\Delta = V$.

The determination of the Sp-orbits of V depends on the ideal structure of R. The simplest case, albeit an important one, occurs when R is principal

2.6.1 Lemma Suppose that R is principal. Then V decomposes into $l+1$ orbits under the action of Sp, namely

$$V \setminus \mathrm{m}V,\ \mathrm{m}V \setminus \mathrm{m}^2V, \ldots, \mathrm{m}^{l-1}V \setminus \mathrm{m}^lV,\ \mathrm{m}^lV = \{0\}.$$

Proof: This is consequence of Corollary 2.2.3 and the fact that R is a local principal ring. □

2.6.2 Lemma (a) If $I \subseteq J$ are ideals of R then the map

$$O(JV) \setminus O(IV) \ni O_v \to O_{v+IV} \in O(JV/IV) \setminus \{0\} \tag{2.22}$$

is an epimorphism.

(b)

$$o(JV/IV) \leq o(JV) - o(IV) + 1.$$

(c)

$$o(\mathrm{m}V) = o(V) - 1.$$

Suppose that R contains a unique minimal ideal min amongst all non-zero ideals of R. Then

(d)

$$o(\mathrm{min}V) = 2.$$

(e)

$$o(IV/\mathrm{min}V) = o(IV) - o(\mathrm{min}V) + 1 \tag{2.23}$$

for all non-zero ideals I of R.

Proof:

(a) This follows immediately from the definition of the objects involved.

(b) Consequence of (a).

(c) Consequence of Corollary 2.2.3.

(d) View $\mathrm{min}V$ as a symplectic space over F_q and then apply Corollary 2.2.3.

(e) A moment of reflexion reveals that (2.23) is equivalent to the following statements:

$$\text{the map (2.22) is injective,}$$

$$O_{w+\mathrm{min}V} = O_{v+\mathrm{min}V} \Rightarrow O_w = O_v \text{ for all } v, w \in IV \setminus \mathrm{min}V,$$

$$w \sim v + u \Rightarrow w \sim v \text{ for all } v, w \in IV \setminus \mathrm{min}V,\ u \in \mathrm{min}V,$$

$$v + u \sim v \text{ for all } v \in IV \setminus \mathrm{min}V,\ u \in \mathrm{min}V. \tag{2.24}$$

We proceed to prove (2.24). The case $I = \mathrm{min}$ is vacuously true, while the case $u = 0$ is trivial. Denote by m a fixed generator of (the necessarily principal ideal) min. Then $0 \neq u \in \mathrm{min}V$ can be written in the form $u = \mathrm{m}x$ for some $x \in \mathcal{P}$. Extend $e_1 = x$ to a

symplectic basis $\{e_1, ..., e_{2n}\}$ of V by means of Lemma 2.2.2 and write $v = r_1e_1 + ... + r_{2n}e_{2n}$. Three case may arise:

Case A. $r_{n+1} \neq 0$. Since $\mathbf{m} \in \min \subseteq (r_{n+1})$ we have $\mathbf{m} = tr_{n+1}$ for some $t \in R$. Then

$$\rho_{t,e_1}(v) = v + t\langle e_1, v\rangle e_1 = v + tr_{n+1}e_1 = v + u,$$

whence $v \sim v + u$.

Case B. $r_{n+1} = 0$ and $r_1 \in I \setminus \min$. Since r_1 does not belong to the annihilator $\min$ of $\mathfrak{m}$ we can choose $t \in \mathfrak{m}$ such that $r_1t \neq 0$. Then

$$\rho_{t,e_{n+1}}(v) = v + t\langle e_{n+1}, v\rangle e_{n+1} = v - r_1te_{n+1} = w \tag{2.25}$$

and

$$\rho_{t,e_{n+1}}(u) = u + t\langle e_{n+1}, u\rangle e_{n+1} = u + t\mathbf{m}\langle e_{n+1}, e_1\rangle e_{n+1} = u. \tag{2.26}$$

Making use of (2.25) and (2.26) in conjunction with Case A applied to w we discover that

$$v \sim w \sim w + u \sim v + u.$$

Case C. $r_{n+1} = 0$, $r_1 \in \min$ and $r_i \in I \setminus \min$ for some $i \neq 1, n+1$. Again, we choose $t \in \mathfrak{m}$ so that $r_it \neq 0$. Without loss of generality assume that $i > n$. Then

$$\begin{aligned}\rho_{t,e_{n+1}+e_{i-n}}(v) &= v + t\langle e_{n+1} + e_{i-n}, v\rangle(e_{n+1} + e_{i-n}) \\ &= v + t\langle e_{i-n}, v\rangle(e_{n+1} + e_{i-n}) \\ &= v + tr_ie_{n+1} + tr_ie_{i-n} = w\end{aligned}$$

and

$$\rho_{t,e_{n+1}+e_{i-n}}(u) = u + t\langle e_{n+1} + e_{i-n}, \mathbf{m}e_1\rangle(e_{n+1} + e_{i-n}) = u.$$

As above, this implies that

$$v \sim w \sim w + u \sim v + u.$$

□

2.7 Passage from the local to the general case

Most of the material developed in the previous sections goes through in the general case with no or obvious modifications. This will be used implicitly in what follows. We proceed to explain this phenomenon.

Given an ideal I of R we shall adopt the following notational conventions:

$$R_I = R/I, \quad V_I = V/IV, \quad r_I = r + IR, \quad v_I = v + IV, \quad \langle v_I, w_I \rangle_I = \langle v, w \rangle,$$

$$\mathrm{Sp}_I = \mathrm{Sp}(R_I, V_I, \langle\ ,\ \rangle_I), \quad H_I = (R_I, V_I, \langle\ ,\ \rangle_I), \quad h_I = (r_I, v_I) \text{ and } g_I v_I = (gv)_I,$$

for all $r \in R$, $v, w \in V$ and $g \in \mathrm{Sp}$.

If the ideal I is clear from the context we shall write

$$\overline{R} = R_I, \quad \overline{V} = V_I, \text{ etc.} \tag{2.27}$$

The symplectic space $(V, \langle\ ,\ \rangle)$ over a general ring $R = R_1 \times ... \times R_t$ can be studied by transporting properties from the corresponding spaces associated to its local components R_i. Set $I_j = \prod_{i \neq j} R_i$ and produce symplectic bases of $(V_{I_j}, \langle\ ,\ \rangle_{I_j})$, $1 \leq j \leq t$, as explained in Lemma 2.2.2. We then obtain a uniquely determined symplectic basis of $(V, \langle\ ,\ \rangle)$, much like in the Chinese remainder theorem. Thus, every symplectic space has a symplectic basis.

Similarly, the study of symplectic groups over $R = R_1 \times ... \times R_t$ can be reduced to the local case. More precisely, we have

2.7.1 Proposition The natural map

$$\mathrm{Sp}_{2n}(R) \ni g \mapsto (g_{I_1}, ..., g_{I_t}) \in \mathrm{Sp}_{2n}(R_1) \times ... \times \mathrm{Sp}_{2n}(R_t) \tag{2.28}$$

is a group isomorphism.

Proof: Since $\overline{\rho_{r,x}} = \rho_{\overline{r},\overline{x}}$, Proposition 2.2.6 shows that (2.28) must be an epimorphism. Its kernel is, by definition, $\cap_{1 \leq j \leq t} \mathrm{Sp}(I_j) = \langle 1 \rangle$. □

2.7.2 Corollary $\mathrm{Sp}_{2n}(R)$ is generated by $(\rho_{r,x})_{r \in R, x \in V}$.

2.7.3 Corollary Let I be an ideal of R. Then the natural map $\mathrm{Sp} \ni g \mapsto \overline{g} \in \overline{\mathrm{Sp}}$ is an epimorphism with kernel $\mathrm{Sp}(I)$.

Chapter 3

Technical Results

3.1 A generalized Legendre symbol

A system to detect the Number of Sign Changes, or NSC-system, is a pair (G, E), where E is a set being acted upon by the groups G and $\{\pm 1\}$ in such a way that these actions commute and -1 does not have any fixed points in E. A moiety of E is then a subset I of E that contains precisely one element out of every pair $\{x, -x\}$ of elements of E; here $-x = (-1)x$. Given $k \in G$, let $I_k = \{i \in I \mid ki \in -I\}$ and define the map $\mu(G, E)$ by means of

$$G \ni k \to (-1)^{|I_k|} \in \{\pm 1\}.$$

3.1.1 Lemma The map $\mu(G, E)$ is a group homomorphism independent of the choice of I.

Proof:

Independence. Let I and J be moieties of E. We shall show that the maps corresponding to I and J are equal if I and J differ in precisely one pair $\{i, -i\}$; here $i \in I$ and $-i \in J$. The result then follows by recurrence. Let $k \in G$. Several cases arise:

- $ki = i$. Then $I_k = J_k$.
- $ki = -i$. Then $I_k \setminus \{i\} = J_k \setminus \{-i\}$ and $i \in I_k$, $-i \in J_k$, whence $|I_k| = |J_k|$.
- $ki \neq \pm i$. Then $k^{-1}i \neq \pm i$ and $I_k \setminus \{i, -k^{-1}i\} = J_k \setminus \{-i, k^{-1}i\}$.

Suppose that $i \in I_k$. Then $-i \notin J_k$ because $ki \notin J$. If $-k^{-1}i \in I$ then $i, -k^{-1}i \in I_k$ but $-i, k^{-1}i \notin J_k$ because $k^{-1}i \notin J$, whence $|I_k| = |J_k| + 2$. If $-k^{-1}i \notin I$ then $k^{-1}i \in J_k$, whence $|I_k| = |J_k|$.

Suppose finally that $i \notin I_k$. Then $|I_k| = |J_k|$ if $-k^{-1}i \in I$ and $|J_k| = |I_k| + 2$ if $-k^{-1}i \notin I$, as above. Thus $(-1)^{|I_k|} = (-1)^{|J_k|}$, as claimed.

Homomorphism. Consider the polynomial ring $T = \mathbf{Z}[(X_a)_{a \in E}]$. Given $k \in G$ consider the automorphism of T given by $X_a \mapsto X_{ka}$. This gives a group homomorphism from G into $\mathrm{Aut}(T)$, and we denote the action of $k \in G$ on $P \in T$ by ${}^kP$. Let I be a moiety of E and $P = \prod_{i \in I}(X_i - X_{-i}) \in T$. Then ${}^kP = \mu(G, E)(k)P$, whence

$$\mu(G, E)(kk') = \mu(G, E)(k)\mu(G, E)(k'). \tag{3.1}$$

□

3.1.2 Question What is $\mu(G, E)$?

As a first example, let Ω be a finite set and $E = \{(x, y) \mid x, y \in \Omega \text{ and } x \neq y\}$. Let $G = Sym(\Omega)$ and $\{\pm 1\}$ act on E by means of $k(x, y) = (kx, ky)$ and $-1(x, y) = (y, x)$. Then $\mu(G, E)$ is the sign homomorphism.

Observe that if G_0 is contained in the kernel of the given permutation representation $G \to Sym(E)$ then $\mu(G/G_0, E)(\overline{k}) = \mu(G, E)(k)$, since $I_k = I_{\overline{k}}$ for all $k \in G$ and corresponding $\overline{k} \in G/G_0$. It can thus be assumed that the action of G on E is faithful and, a fortiori, that G itself is finite.

Also, if $E_1, ..., E_d$ are mutually disjoint and exhaustive subsets of E which are stable under G and -1 then

$$\mu(G, E)(k) = \prod_{1 \leq j \leq d} \mu(G, E_j)(k) \tag{3.2}$$

for all $k \in G$. One could then assume that G acts transitively on E.

We shall find it necessary to answer Question 3.1.2 in the following context. Suppose that T is a finite ring with 1 such that $2 = 1 + 1$ is invertible. Let A be a T-module and E a T^*-stable subset of A. Then $(T^*, E \setminus \{0\})$ is an NSC-system relative to the action of

$-1 \in T^*$. If $A = T$ affords the left regular representation we shall write $\mu(T^*)$ to mean $\mu(T^*, T \setminus \{0\})$.

We are particularly interested in $\mu(\mathrm{GL}(A), A\setminus\{0\})$, when A is free with basis $\{e_1, ..., e_d\}$ over R, and $\mu(R^*)$, henceforth denoted by μ. The former problem can easily be reduced to the latter, which in turn can be reduced to the local case, a complete answer for which is given in Theorem 3.1.4 below. The reason for our interest is that $\mu(\mathrm{GL}(A), A \setminus \{0\})$ is inevitably involved in the determination of the Weil representation of $\mathrm{Sp}_{2n}(R)$.

Identify $\mathrm{GL}(A)$ with $\mathrm{GL}_d(R)$ by means of the given basis. In order to determine $\mu(\mathrm{GL}(A), A \setminus \{0\})$ it suffices to find its action on each $A(k) = \mathrm{diag}(k, 1, ..., 1)$, $k \in R^*$ (Lemma 2.3.10). Given a moiety I of $R \setminus \{0\}$ define a moiety $U = U(I)$ of $A \setminus \{0\}$ by letting $U_i = \{\sum_{1 \le j \le i} r_j e_j \mid r_j \in R\,, r_i \in I\}$ and $U = \cup_{1 \le i \le n} U_i$. Then

$$u \in U_{A(k)} \Leftrightarrow A(k)u \in -U \Leftrightarrow u = re_1$$

for a unique $r \in I_k$. Thus $\mu(\mathrm{GL}(A), A \setminus \{0\})(A(k)) = \mu(k) = \mu(\det A(k))$, whence

$$\mu(\mathrm{GL}(A), A \setminus \{0\})(g) = \mu(\det g) \tag{3.3}$$

for all $g \in \mathrm{GL}(A)$. This takes care of the first reduction.

3.1.3 Lemma Suppose that $R = R_1 \times ... \times R_t$, and write $\mu_i = \mu(R_i^*)$. Then

$$\mu(k_1, ..., k_t) = \mu_1(k_1)...\mu_t(k_t)$$

for all units $(k_1, ..., k_t) \in R$

Proof: By recurrence, it suffices to prove the statement when $t = 2$. Let I_i be a moiety of $R_i \setminus \{0\}$, $i = 1, 2$. Consider the mutually disjoint and exhaustive R^*-stable subsets $E_1 = R_1 \setminus \{0\}$ and $E_2 = R_1 \times (R_2 \setminus \{0\})$ of $R \setminus \{0\}$, with moieties I_1 and $R_1 \times I_2$, respectively. Then (3.2) gives $\mu(k_1, k_2) = \mu(R, E_1)(k_1, k_2)\mu(R, E_2)(k_1, k_2)$. Since $|R_i|$ is odd, we have $\mu(R, E_i)(k_1, k_2) = \mu_i(k_i)$, $i = 1, 2$, as desired. □

This takes care of the second reduction.

3.1.4 Theorem If R is local then $\mu = \left(\frac{\bullet}{R}\right)^{d_R}$. In other words,

$$\mu = \begin{cases} \text{trivial} & \text{if } d_R \text{ is even} \\ \left(\frac{\bullet}{R}\right) & \text{if } d_R \text{ is odd.} \end{cases} \tag{3.4}$$

Proof: By induction on $|R|$. If $R = F_q$ the result was proved by Gauss ([Rib72], page 52). This covers the base case. Suppose that R is not a field and the result to be true for all rings of smaller size than R. Let U be a minimal ideal of R, which is a one-dimensional vector space over F_q. In view of (3.1) and the truth of (3.4) in the field case we have

$$\mu(R^*, U \setminus \{0\})(k) = \left(\frac{\hat{k}}{q}\right) = \left(\frac{k}{R}\right), \tag{3.5}$$

where $\hat{k} \in F_q$ is the canonical image of $k \in R^*$. Let $\overline{R} = R/U$ and let $P : R \to \overline{R}$ be the canonical projection. Given a moiety $\overline{J}$ of $\overline{R} \setminus \{0\}$ let $J = P^{-1}(\overline{J})$. Then J is a moiety of $E = J \cup -J$, which is an R^*-stable set that contains all elements of R not belonging to U. Given $k \in R^*$, set $\overline{k} = P(k)$. Then

$$t \in J_k \Leftrightarrow kt \in -J \Leftrightarrow \overline{kt} \in -\overline{J} \Leftrightarrow \overline{t} \in \overline{J}_{\overline{k}}.$$

Thus $|J_k| = |U||\overline{J}_{\overline{k}}|$, whence

$$\mu(R^*, E)(k) = \left(\frac{\overline{k}}{\overline{R}}\right)^{d_{\overline{R}}} = \left(\frac{k}{R}\right)^{d_{\overline{R}}}, \tag{3.6}$$

by inductive hypothesis and Lemma 2.2.1. Note that $d_R = d_{\overline{R}} + 1$.

Since E and $U \setminus \{0\}$ are R^*-stable disjoint subsets whose union is equal to $R \setminus \{0\}$, (3.2), (3.5) and (3.6) give

$$\mu(k) = \mu(R^*, E)(k)\mu(R^*, U \setminus \{0\})(k) = \left(\frac{k}{R}\right)\left(\frac{k}{R}\right)^{d_{\overline{R}}} = \left(\frac{k}{R}\right)^{d_R}.$$

□

3.2 Quadratic sums

A complex linear character of R^+ (or an additive linear character of R) is a group homomorphism $\lambda : R^+ \to \mathbf{C}^*$. Since $cr = 0$ for all $r \in R^+$, the image of λ lies in F^*. We shall say that λ is primitive if its kernel does not contain any non-zero ideals of R.

To any linear character λ, whether primitive or not, we can associate a quadratic sum

$$\sum(\lambda) = \sum_{r \in R} \lambda(r^2).$$

The aim of this section is to determine $\sum(\lambda)$ as explicitly as possible. One reason to do this is that these quadratic sums are unavoidably involved in the determination of the Weil representations. An alternative approach will be taken in Section 5.7.

A closely related concept is that of a Gauss sum $\sum(\chi, \lambda)$, where χ is a multiplicative linear character of R; that is, a group homomorphism $\chi : R^* \to \mathbf{C}^*$. The corresponding Gauss sum is then defined by

$$\sum(\chi, \lambda) = \sum_{k \in R^*} \chi(k)\lambda(k).$$

The Gauss sums $\sum(\chi, \lambda)$ are completely described in [Lam53]. The computation of both $\sum(\lambda)$ and $\sum(\chi, \lambda)$ can be reduced first to the case that R is local and then to the case when λ and χ are both primitive. To say that χ is primitive means that its kernel does not contain any subgroup of the form $1 + I$, where I is an ideal of R.

It is easy to see that in the field case $R = F_q$ one has

$$\sum(\chi, \lambda) = \sum(\lambda), \tag{3.7}$$

whenever λ is not trivial (and hence primitive) and χ is the Legendre symbol $\left(\frac{\bullet}{q}\right)$. It is false however, in general, that given any primitive λ there exists a χ such that (3.7) holds (e.g. $R = \mathbf{Z}/9\mathbf{Z}$). What it is true is that the values $\sum(\chi, \lambda)$ and $\sum(\lambda)$ all lie in the same circumference of radius $\sqrt{|R|}$, for any primitive λ and χ.

We proceed to establish the aforementioned reductive steps in the computation of $\sum(\lambda)$. Denote by λ_i be the additive linear character of the local component R_i obtained by restricting λ to R_i. We then have

3.2.1 Lemma

$$\sum(\lambda) = \sum(\lambda_1) \ldots \sum(\lambda_t)$$

Proof: This follows from the very definitions of the objects involved. □

Assume henceforth that R is a local ring. Consider next the largest ideal $I = I_\lambda$ contained in the kernel of λ; such ideal exists because the sum of finitely many ideals contained in Ker λ is also contained in Ker λ. Adopt the notation of (2.27) for $I = I_\lambda$. We can define a primitive linear character $\widehat{\lambda}$ of $\overline{R}^+$ as follows:

$$\widehat{\lambda}(\overline{r}) = \lambda(r). \tag{3.8}$$

Then $\sum(\lambda)$ and $\sum(\widehat{\lambda})$ are related by

3.2.2 Lemma $\sum(\lambda) = |I| \sum(\widehat{\lambda})$

Proof:

$$\sum(\lambda) = \sum_{r \in \mathcal{T}(R/I)} \sum_{s \in I} \lambda((r+s)^2) = \sum_{r \in \mathcal{T}(R/I)} \lambda(r^2) \sum_{s \in I} \lambda(2rs + s^2)$$
$$= |I| \sum_{r \in \mathcal{T}(R/I)} \lambda(r^2) = |I| \sum(\widehat{\lambda}).$$

□

This takes care of the promised reductions. We shall henceforth assume that λ is a primitive linear character of R^+. This assumption should not be taken lightly, since it is definitely false that every local ring R possesses a primitive linear character. In other words, the primitivity of λ forces R to belong to a class of rings strictly smaller than the universe of all local rings. We proceed to determine this class.

We shall say that R is irreducible if (0) cannot be written as the intersection of non-zero ideals; that is, if R possesses a unique minimal ideal min amongst all non-zero ideals of R. An ideal I will be said to be irreducible if R/I is an irreducible ring.

3.2.3 Proposition R possesses a primitive additive linear character if and only if R is irreducible.

Proof:

Sufficiency: If $R = F_q$ is a field then any non-trivial linear character of R^+ is primitive. Otherwise the number of non-primitive linear characters of R^+ is equal to the number

$|R/\mathrm{min}|$ of linear characters of $(R/\mathrm{min})^+$. Thus $|R| - |R/\mathrm{min}| > 0$ linear characters of R^+ are primitive.

Necessity: If R is not a field, let I and J be different minimal ideals of R, neither of which is equal to (0) or R. Then $\mathrm{m}I = \mathrm{m}J = (0)$ and $K = I \oplus J$ is a vector space of dimension two over F_q. A proper subset L of K is an ideal of R if and only if L is an F_q-line (through the origin).

Let λ be a primitive linear character of R^+. Since K is an elementary abelian p-group, $\mathrm{Im}\lambda \subseteq \mathbf{C}^*$ must be isomorphic to C_p. It follows that $\mathrm{Ker}\,\lambda \cap K$ is a hyperplane of K, viewed as a vector space over F_p.

Denote by PK the set of all F_q-lines in K and by HK the set of all F_p-hyperplanes of K. Observe that $|\mathrm{P}K| = q + 1$ and $|\mathrm{H}K| = \frac{q^2-1}{p-1}$. Given any $L \in \mathrm{PK}$ denote by HK_L the set of all F_p-hyperplanes of K containing L. The cardinality of HK_L is equal to the number of F_p-lines in a vector space of dimension one over F_q, that is, $\frac{q-1}{p-1}$. Observe that the union $\cup_{L\in\mathrm{P}K}\mathrm{H}K_L$ is disjoint, since the sum of any two F_q-lines in K equals K. Thus $|\cup_{L\in\mathrm{P}K}\mathrm{H}K_L| = \frac{q^2-1}{p-1} = |\mathrm{H}K|$, thereby proving that every F_p-hyperplane of K, and in particular $\mathrm{Ker}\,\lambda \cap K$, contains an F_q-line of K. This contradicts the primitivity of λ. □

Thus, by supposing that λ is primitive we are automatically assuming that R is irreducible. The next result produces all primitive additive linear characters of R.

3.2.4 Lemma Denote by $\widehat{R^+}$ the group of all linear characters of R^+. Then the map $R^+ \ni r \to \lambda[r] \in \widehat{R^+}$, where $\lambda[r](r') = \lambda(rr')$, is a group isomorphism and all the primitive linear characters of R^+ are of the form $\lambda[k]$, $k \in R^*$.

Proof: The first assertion is consequence of the primitivity of λ and the fact that $|R^+| = |\widehat{R^+}|$ is finite. Given $r \in R$, either $\mathrm{Ann}(r)$ is zero or not depending on whether r is a unit or not, which proves the second assertion. □

3.2.5 Definition We shall say that λ and $\lambda[k]$ are equivalent if $k \in R^*$ is a square.

This breaks up the set of all primitive linear characters of R^+ into two equivalence classes.

We resume our discussion about quadratic sums. The field case will not be treated

since it is already known. In fact, if $R = F_q$ then

$$\sum(\lambda) = \pm\sqrt{\left(\frac{-1}{q}\right)q} \tag{3.9}$$

and

$$\sum(\lambda[k]) = \left(\frac{k}{q}\right)\sum(\lambda) \tag{3.10}$$

for all $k \in F_q^*$. Moreover, the sign in (3.9) can be determined ([Lan70], chapter 4).

Suppose henceforth that R is not a field. We shall determine $\sum(\lambda)$ either by itself, if d_R is even, or in terms of the quadratic sum associated to a primitive linear character $\overline{\lambda}$ of F_q^+, if d_R is odd. We proceed to construct the character $\overline{\lambda}$. As we shall see, the equivalence class of $\overline{\lambda}$ depends only on λ and not on the actual way we define it.

Since $\mathfrak{m}\mathfrak{i}\mathfrak{n}$ is one-dimensional over $R/\mathfrak{m}$, it is generated by any of its non-zero elements. Fix one of them, say $\mathbf{m}$, and define $\overline{\lambda}$ by means of (3.8), as follows:

$$\overline{\lambda} = \widehat{\lambda[\mathbf{m}]},$$

that is,

$$\overline{\lambda}(\overline{r}) = \lambda(r\mathbf{m}). \tag{3.11}$$

We record some basic properties related to this construction.

3.2.6 Lemma Let $k \in R^*$ and set $\overline{k} = k + \mathfrak{m} \in F_q$. Then

(a)

$$\overline{\lambda}[\overline{k}] = \overline{\lambda[k]} \tag{3.12}$$

(b)

$$\sum(\lambda[k\mathbf{m}]) = \left(\frac{k}{R}\right)\sum(\lambda[\mathbf{m}]) \tag{3.13}$$

Proof:

(a) This is clear.

(b) In view of Lemma 3.2.2, Lemma 2.2.1(c), (3.10) and (a) we have

$$\sum(\lambda[k\mathbf{m}]) = |\mathbf{m}| \sum(\widehat{\lambda[k\mathbf{m}]}) = |\mathbf{m}| \sum(\overline{\lambda}[k]) = |\mathbf{m}| \sum(\overline{\lambda}[k])$$
$$= \left(\frac{\overline{k}}{q}\right) |\mathbf{m}| \sum(\overline{\lambda}) = \left(\frac{k}{R}\right) \sum(\lambda[\mathbf{m}]).$$

□

In order to make progress we need to record some subtle properties enjoyed by every irreducible ring. If I, J are ideals of R we shall denote by $(I : J) = \{r \in R \,|\, rJ \subseteq I\}$ the conductor of J into I. Then in an irreducible ring we have

$$((0) : ((0) : I)) = I \tag{3.14}$$

and

$$|R| = |I||((0) : I)| \tag{3.15}$$

A proof of (3.14) can be found in [ZS58], chapter IV, § 16. For a historical perspective see [Kru68]. A ring-theoretical proof of (3.15) is given in [Lam53], page 159. An independent character-theoretical proof of both (3.14) and (3.15) will be given in Section 4.1, as a consequence of the very existence of the Schrödinger character.

The following observation is quite useful.

3.2.7 Lemma If I, J are ideals of R and $J = ((0) : I)$ then $(I : J) = ((0) : J^2)$.

Proof:

$$x \in (I : J) \Leftrightarrow xJ \subseteq I \Leftrightarrow xJ^2 = (0) \Leftrightarrow x \in ((0) : J^2).$$

□

Another property of irreducible rings proved in [ZS58], chapter IV, § 16 is the following:

3.2.8 Proposition An ideal I of an irreducible ring R is irreducible if and only if $J = ((0) : I)$ is a principal ideal.

Proof: Suppose that I is irreducible and let $\overline{\lambda}$ be a primitive linear character of R/I. Inflate λ to a linear character of R. According to Lemma 3.2.4 this inflated character

must be equal to $\lambda[r]$ for some $r \in R$. The statement that $\overline{\lambda}$ is primitive is equivalent to $((0) : (r)) = I$, whence (3.14) gives $J = (r)$, as claimed.

Conversely, if $J = (r)$ then $((0) : (r)) = I$ and therefore $\overline{\lambda}(x + I) = \lambda(rx)$ defines a primitive linear character of R/I, as required. □

A pair of ideals (I, J) such that $I^2 = (0)$ and $J = ((0) : I)$ will be referred to as an A-pair. Thus $I \subseteq J$ and $((0) : J) = I$ for any A-pair (I, J). Should R be principal then its A-pairs are precisely $(\mathfrak{m}^{l-i}, \mathfrak{m}^i)$, $0 \leq i \leq \lfloor l/2 \rfloor$.

The set of all A-pairs can be ordered by declaring $(I, J) \leq (I_1, J_1)$ whenever either of the following equivalent conditions holds:

$$I \subseteq I_1, \quad J_1 \subseteq J, \quad I \subseteq I_1 \subseteq J_1 \subseteq J$$

The only minimal A-pair is the trivial one, namely $(0, R)$. The maximal ones need not be unique.

We shall say that an A-pair (I, J) is a B-pair if $(I : J)$ is equal to R or $\mathfrak{m}$. We can reformulate the definition of B-pair as follows: it is an A-pair (I, J) such that either $J^2 = (0)$, in which case $I = J$, or else $J^2 = \min$. This follows immediately from Lemma 3.2.7 and the fact that $\min = ((0) : \mathfrak{m})$. Should R be principal then its only B-pair is $(\mathfrak{m}^{\lceil l/2 \rceil}, \mathfrak{m}^{\lfloor l/2 \rfloor})$.

Every irreducible ring has a B-pair. In fact, we have the following result due to Lamprecht ([Lam53], page 162).

3.2.9 Proposition Every maximal A-pair (I, J) in an irreducible ring is a B-pair.

Proof: In view of the above discussion we need to prove that either $J^2 = (0)$ or $J^2 = \min$ holds. Suppose that $J^2 \neq (0)$. If $x^2 \in \min$ for all $x \in J$ then

$$2x_1x_2 = (x_1 + x_2)^2 - x_1^2 - x_2^2 \in \min$$

for all $x_1, x_2 \in J$, whence $J^2 = \min$. We proceed to show that no $x \in J$ satisfies $x^2 \in \min$. Indeed, if such x exists then there must also exist a $y \in \mathfrak{m}$ such that $0 \neq yx^2 \min$. Since $y \in \mathfrak{m}$ and $yx^2 \in \min$ we have

$$0 = y(yx^2) = (yx)^2. \tag{3.16}$$

In light of (3.16) and the fact that xy belongs to J we have

$$(I + (xy))^2 = (0),$$

whence $xy \in I$ by the maximality of I. Since $x \in J$ we deduce that $x^2y = 0$, against the choice of y. □

Given a B-pair (I, J), let $d_{I,J} = \dim_{F_q} J/I$. If (I_1, J_1) is an A-pair which is preceded a B-pair (I, J) then (I_1, J_1) is itself a B-pair and $d_{I,J} = d_{I_1,J_1}$ if and only if $(I, J) = (I_1, J_1)$. This follows from $I \subsetneq I_1 \subsetneq J_1 \subsetneq J$. In general, neither $(I, J) = (I_1, J_1)$ nor $d_{I,J} = d_{I_1,J_1}$ need to hold. However, we do have

3.2.10 Lemma The parity of $d_{I,J}$ is an invariant of the ring. In other words, if (I, J) and (I_1, J_1) are B-pairs, then $d_{I,J} \equiv d_{I_1,J_1} \mod 2$

Proof: We have

$$q^{d_R} = |R| = |J||I| = q^{d_{I,J}}|I|^2$$

due to (3.15). Now apply Lemma 2.2.1(a). □

Lemma 3.2.10 establishes a clear dichotomy amongst irreducible rings; as we shall see, $\sum(\lambda)$ is subtle enough to distinguish between these classes. Moreover, there are two essentially different cases that arise when d_R is even, namely whether R has an ideal which is its own annihilator or not, and these can also be detected by $\sum(\lambda)$. Indeed, each B-pair comes equipped with a natural structure of orthogonal space over F_q, and the type of orthogonal space thus arising is, in a sense, independent of the actual choice of the B-pair. The value of $\sum(\lambda)$ ultimately depends on the type of orthogonal space attached to the maximal B-pairs of R.

Our presentation, thus, requires a basic knowledge of orthogonal spaces over finite fields of odd characteristic. We introduce some elementary definitions and refer the reader to [Jac85], [Wan93] for details. An orthogonal space over F_q is a pair $(Q, (,))$ where Q is a finite dimensional vector space over F_q and $(,)$ is a non-degenerate symmetric bilinear form on Q. For convenience, we shall allow $d = \dim_{F_q} Q$ to be zero. A subspace Q_0 of Q is totally isotropic if $(Q_0, Q_0) = 0$. The Witt index ν of the space $(Q, (,))$ is the common

dimension of all maximal totally isotropic subspace. There are precisely four types of orthogonal spaces, if we disregard the dimension of the space and only take into account its parity. They can be defined as follows:

3.2.11 Proposition There is a basis $\{x_1, ..., x_d\}$ of Q where the matrix of $(,)$ is of one, and only one, of the following four types:

$$\text{type } 0 = \left(\begin{array}{c|c} 0 & 1_\nu \\ \hline 1_\nu & 0 \end{array}\right)$$

or

$$\text{type } 2 = \left(\begin{array}{c|c|c|c} 0 & 1_\nu & 0 & 0 \\ \hline 1_\nu & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & b \end{array}\right), \quad \left(\frac{-b}{q}\right) = -1$$

if d is even, and

$$\text{type } 1 = \left(\begin{array}{c|c|c} 0 & 1_\nu & 0 \\ \hline 1_\nu & 0 & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$$

or

$$\text{type } 3 = \left(\begin{array}{c|c|c} 0 & 1_\nu & 0 \\ \hline 1_\nu & 0 & 0 \\ \hline 0 & 0 & b \end{array}\right), \quad \left(\frac{b}{q}\right) = -1$$

if d is odd. The four matrices defined above are not cogredient. Here 1_ν denotes the $\nu \times \nu$ identity matrix.

Proof: See [Wan93], chapter 6. □

We shall say that $(Q, (,))$ is of type 0, 1, 2 or 3 depending on whether Q affords a basis where $(,)$ looks like a matrix of one these types.

3.2.12 Proposition Let (I, J) be any B-pair and $d = d_{I,J}$. Then

$$J/I \times J/I \ni (\overline{x}, \overline{y}) \mapsto xy \in \min = F_q\mathbf{m}$$

defines an orthogonal space $(J/I, (,))$ of dimension d over F_q.

Proof: Since $IJ = II = (0)$, $(,)$ is a well-defined symmetric bilinear form. It is non-degenerate because if $\overline{x} \neq 0$ then $x \notin I = \mathrm{Ann}(J)$ and there exists $y \in J$ such that $(\overline{x}, \overline{y}) = xy \neq 0$. □

3.2.13 Lemma Let (I, J) be a B-pair. Set $d = d_{I,J}$ and let $\{x_1, ..., x_d\}$ be a basis of J/I over F_q. Then

$$\sum(\lambda) = |I| \sum_{a_1,...,a_d \in F_q} \lambda((a_1x_1 + ... + a_dx_d)^2). \tag{3.17}$$

Proof:

$$\sum(\lambda) = \sum_{r \in \mathcal{T}(R/I)} \sum_{s \in I} \lambda((r+s)^2) = \sum_{r \in \mathcal{T}(R/I)} \lambda(r^2) \sum_{s \in I} \lambda(2rs). \tag{3.18}$$

For a fixed $r \in R$, the map $I \ni s \mapsto \lambda(2rs) \in F^*$ is a linear character of I. Since λ is primitive, this is the trivial character if and only if $r \in \mathrm{Ann}(I) = J$. Thus

$$\sum_{s \in I} \lambda(2rs) = \begin{cases} 0 & \text{if } r \notin J \\ |I| & \text{otherwise} \end{cases}$$

Therefore (3.18) can be rewritten as

$$|I| \sum_{r \in \mathcal{T}(J/I)} \lambda(r^2) = |I| \sum_{a_1,...,a_d \in F_q} \lambda((a_1x_1 + ... + a_dx_d)^2),$$

as claimed. □

To avoid unnecessary repetitions we shall say that R is homogeneous if it possesses an ideal which is its own annihilator. The theory of Weil representations of $\mathrm{Sp}_{2n}(R)$ for homogeneous rings R is substantially simpler than in the general case.

3.2.14 Theorem Let R be an irreducible ring and λ a primitive linear character of R^+. Then

$$\sum(\lambda) = \begin{cases} \sqrt{|R|} & \text{if } d_R \text{ is even and } R \text{ is homogeneous} \\ -\sqrt{|R|} & \text{if } d_R \text{ is even but } R \text{ is not homogeneous} \\ \sqrt{|R|/q}\sum(\overline{\lambda}) & \text{if } d_R \text{ is odd.} \end{cases} \tag{3.19}$$

If d_R is odd, we define $\overline{\lambda}$ as in (3.11) by letting $\mathbf{m} = x^2$ for any $x \in J \setminus I$ and any maximal B-pair (I, J) of R. This is a canonical choice that leads to the same equivalence class of $\overline{\lambda}$, regardless of the choices of x and (I, J).

The following relations are satisfied:

$$\sum(\lambda) = \pm\sqrt{\mu(-1)|R|} \tag{3.20}$$

and

$$\sum(\lambda[k]) = \mu(k)\sum(\lambda) \tag{3.21}$$

for all units $k \in R$.

If (I, J) is any maximal B-pair then the dimension $d = d_{I,J}$ is an invariant of R. In fact:

$$d = \begin{cases} 0 & \text{if } d_R \text{ is even and } R \text{ is homogeneous} \\ 2 & \text{if } d_R \text{ is even but } R \text{ is not homogeneous} \\ 1 & \text{if } d_R \text{ is odd.} \end{cases}$$

Moreover, the isomorphism type of the orthogonal space $(J/I, (,))$ is also an invariant of the ring. In fact, there is a basis of J/I over F_q where $(,)$ looks like

$$\begin{cases} \emptyset & \text{if } d_R \text{ is even and } R \text{ is homogeneous} \\ \begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}, \quad \left(\frac{-b}{q}\right) = -1 & \text{if } d_R \text{ is even but } R \text{ is not homogeneous} \\ (1) & \text{if } d_R \text{ is odd.} \end{cases} \tag{3.22}$$

If d_R is odd we set $\mathbf{m} = x^2$ for any $x \in J \setminus I$. This is a canonical choice that leads to the same isomorphism class of orthogonal space, regardless of the choices of x and (I, J).

Proof: Given any B-pair (I_0, J_0), construct the orthogonal space $(J_0/I_0, (,))$ given in Proposition 3.2.12. We shall consider the natural bijection between the set of ideals I that satisfy $I_0 \subseteq I \subseteq J_0$ and the set of subspaces of J_0/I_0 to be an identification. Under this identification totally isotropic subspaces correspond to ideals of square (0) and the relation $\mathrm{Ann}(I) = J$ corresponds to $I^{\perp} = J$.

Let $\{y_1, ..., y_t\}$ be a basis of J_0/I_0 where $(,)$ looks like one of the matrices of the aforementioned types. Let $I = F_q y_1 \oplus ... \oplus F_q y_\nu$ and $J = I^\perp$. Then

$$I \subseteq J = \begin{cases} I & \text{if } (,) \text{ is of type 0} \\ I + F_q y_{t-1} \oplus F_q y_d & \text{if } (,) \text{ is of type 2} \\ I + F_q y_t & \text{if } (,) \text{ is of type 1} \end{cases}$$

and $J^\perp = I$, which is a maximal totally isotropic subspace of J_0/I_0. Set $d = d_{I,J}$. Three cases arise:

Case 0. $d = 0$. Then Lemma 3.2.13 and (3.15) give

$$\sum(\lambda) = |I| = \sqrt{|R|}.$$

Case 1. $d = 1$. Then J/I has a basis $\{x\}$, where $x^2 \neq 0$, and Lemma 3.2.13 gives

$$\sum(\lambda) = |I| \sum_{a \in F_q} \lambda(a^2 x^2) = |I| \sum(\overline{\lambda}).$$

But (3.15) shows that

$$|R| = |J||I| = q|I|^2,$$

whence

$$\sum(\lambda) = \sqrt{|R|/q} \sum(\overline{\lambda}).$$

Case 2. $d = 2$. Then J/I has a basis $\{x_1, x_2\}$ where $(,)$ looks like $\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}$, $\left(\frac{-b}{q}\right) = -1$. Now (3.17) becomes

$$\begin{aligned} \sum(\lambda) &= |I| \sum_{a_1, a_2 \in F_q} \lambda(a_1^2 \mathbf{m} + a_2^2 b \mathbf{m}) = |I| \sum(\overline{\lambda}) \sum(\overline{\lambda}[b]) \\ &= |I| \left(\frac{b}{q}\right) \sum(\overline{\lambda})^2 = |I| \left(\frac{b}{q}\right) \left(\frac{-1}{q}\right) q \\ &= |I| \left(\frac{-b}{q}\right) q = -|I| q = -\sqrt{|R|} \end{aligned}$$

since $|R| = |J||I| = q^2|I|^2$, due to (3.15).

Since the value of $\sum(\lambda)$ is independent of the choice of maximal B-pair, Lemma 3.2.10 and the above reasoning show that the expressions appearing in (3.19) are exhaustive,

mutually exclusive and do not depend on the choice of (I, J). Thus, neither do any of the alluded objects attached to (I, J). The independence of (3.22) and $\overline{\lambda}$ from x is clear.

Applying Theorem 3.1.4, Lemma 2.2.1(c), (3.10) and (3.12) to (3.19) we see that (3.20) and (3.21) are correct. □

3.2.15 Example Let $R = F_q[s,t]$, subject to the relations $t^2 = bs^2$, $st = 0$, $s^3 = t^3 = 0$; here b belongs to a transversal of F_q^* relative to $(F_q^*)^2$.

Then $R = F_q \oplus F_q s \oplus F_q t \oplus F_q s^2$ and $\mathfrak{m} = (s,t)$, $\min = (s^2) = \mathfrak{m}^2$. Set $I = \min$, $\mathbf{m} = s^2$ and $J = \mathfrak{m}$. Then (I, J) is a B-pair. Let λ be any primitive linear character of R^+ (just set $\lambda(\mathbf{m}) =$ some primitive p-th root of unity). On the basis $\{s,t\}$ of J/I over F_q, $(,)$ looks like $\begin{pmatrix} 1 & 0 \\ 0 & b \end{pmatrix}$. Thus $(,)$ is of type $\begin{cases} 0 & \text{if } \left(\frac{-b}{q}\right) = 1 \\ 2 & \text{otherwise} \end{cases}$.

If $\left(\frac{-b}{q}\right) = 1$, say $a^2 = -b$, then $(s + a^{-1}t)$ is its own annihilator and $\sum(\lambda) = \sqrt{|R|}$, whereas if $\left(\frac{-b}{q}\right) = -1$ then such ideal does not exists and $\sum(\lambda) = -\sqrt{|R|}$.

3.3 Projective versus Ordinary Representations

The goal of this section is to provide the tools needed to establish the existence of the Weil representation. We develop our machinery in a slightly more general scenario that captures the essential features encountered in the latter setting. Thus, we shall let $\mathbb{G}$ be an arbitrary finite group and $\mathbf{P} : \mathbb{H} \to \mathrm{GL}(\mathbf{X})$ a projective representation of $\mathbb{G}$ over an arbitrary field $\mathbb{F}$. The aim is to construct, if possible, an ordinary representation $\mathbf{W} = \mathbf{P}c$ of $\mathbb{G}$ by suitably choosing a correcting factor $c : \mathbb{G} \to \mathbb{F}^*$.

It is not hard to see that if $\mathbf{X}$ possesses $\mathbf{P}$-invariant $\mathbb{F}$-subspaces of coprime dimensions then $\mathbf{P}$ can indeed be corrected to an ordinary representation. The problem is: where should one look for these subspaces, if they exist at all? As shown below, subspaces naturally associated to central elements of $\mathbb{G}$ are good candidates, provided certain relatively mild conditions hold. We are ready to state:

3.3.1 Proposition Suppose that there exist $\mathbf{P}$-invariant $\mathbb{F}$-subspaces $\mathbf{X}_0, ..., \mathbf{X}_t$ of $\mathbf{X}$

whose dimensions $d_0, ..., d_t$ satisfy

$$1 = s_0 d_0 + ... + s_t d_t \tag{3.23}$$

for some integers $s_0, ..., s_t$. Then the function $c : \mathbb{G} \to \mathbb{F}^*$ defined by

$$c(g) = (\det \mathbf{P}(g)|_{\mathbf{X}_0})^{-s_0} ... (\det \mathbf{P}(g)|_{\mathbf{X}_t})^{-s_t} \tag{3.24}$$

is a correcting factor for $\mathbf{P}$. In other words, $\mathbf{W}(g) = \mathbf{P}(g)c(g)$ defines an ordinary representation of $\mathbb{G}$ over $\mathbb{F}$.

Proof: Let f be the factor set corresponding to $\mathbf{P}$. Then taking determinants in

$$\mathbf{P}(g_1)|_{\mathbf{X}_i} \mathbf{P}(g_2)|_{\mathbf{X}_i} = \mathbf{P}(g_1 g_2)|_{\mathbf{X}_i} f(g_1, g_2)$$

we obtain $f^{d_i} = \delta(\nu_i)$, where $\nu_i(g) = \det \mathbf{P}(g)|_{\mathbf{X}_i}$ and $\delta(\nu_i)(g_1, g_2) = \nu_i(g_1)\nu_i(g_2)\nu_i(g_1 g_2)^{-1}$. Thus the factor set of $\mathbf{W} = \mathbf{P}c$ is equal to

$$f\delta(c) = f^{s_0 d_0 + ... + s_t d_t} \delta(\nu_0)^{-s_0} ... \delta(\nu_t)^{-s_t} = (f^{d_0}\delta(\nu_0)^{-1})^{s_0} ... (f^{d_t}\delta(\nu_t)^{-1})^{s_t} = 1.$$

□

3.3.2 Proposition Let z be a central element of $\mathbb{G}$ of order m. Suppose either that $\mathrm{tr}\,\mathbf{P}(z) \neq 0$ or that $\mathbb{G}$ contains no non-trivial cyclic quotient group of order dividing m. Then

$$\mathbf{P}(g)\mathbf{P}(z) = \mathbf{P}(z)\mathbf{P}(g)$$

for all $g \in \mathbb{G}$.

Proof (due to R. Gow; see also [Sze98], Proposition 1): As $\mathbf{P}$ is a projective representation and z is central, it is elementary to check that

$$\mathbf{P}(g)\mathbf{P}(z) = \tau(g)\mathbf{P}(z)\mathbf{P}(g)$$

for all g, where $\tau(g)$ is a non-zero scalar. Thus

$$\mathbf{P}(g)\mathbf{P}(z)\mathbf{P}(g)^{-1} = \tau(g)\mathbf{P}(z).$$

Taking traces, we obtain

$$\mathrm{tr}\,\mathbb{P}(z) = \tau(g)\mathrm{tr}\,\mathbb{P}(z)$$

and thus $\tau(g) = 1$ for all g if $\mathrm{tr}\,\mathbb{P}(z) \neq 0$.

If $\mathrm{tr}\,\mathbb{P}(z) = 0$, we proceed as follows. Given g and h in $\mathbb{G}$, we have

$$\mathbb{P}(g)\mathbb{P}(h) = f(g,h)\mathbb{P}(gh),$$

where f is the factor set associated with $\mathbb{P}$. Now

$$\begin{aligned}\tau(gh)\mathbb{P}(z) &= \mathbb{P}(gh)\mathbb{P}(z)\mathbb{P}(gh)^{-1} \\ &= f(g,h)^{-1}\mathbb{P}(g)\mathbb{P}(h)\mathbb{P}(z)f(g,h)\mathbb{P}(h)^{-1}\mathbb{P}(g)^{-1} \\ &= \tau(g)\tau(h)\mathbb{P}(z).\end{aligned}$$

Thus $\tau : \mathbb{G} \to \mathbb{F}^*$ is a homomorphism.

Since $\mathbb{P}$ is a projective representation and z has order m, it follows easily that

$$\mathbb{P}(z)^m = \alpha I$$

for some $\alpha \in \mathbb{F}$. Thus taking m-th powers,

$$\begin{aligned}\left(\mathbb{P}(g)\mathbb{P}(z)\mathbb{P}(g)^{-1}\right)^m &= \mathbb{P}(g)\mathbb{P}(z)^m\mathbb{P}(g)^{-1} \\ &= \alpha I \\ &= \tau(g)^m\mathbb{P}(z)^m \\ &= \tau(g)^m\alpha I.\end{aligned}$$

Thus $\tau(g)^m = 1$ and it follows that τ is a homomorphism from $\mathbb{G}$ into the group of m-th roots of unity in $\mathbb{F}^*$. In particular,

$$\mathbb{G}/\mathrm{Ker}\,\tau \cong \tau(\mathbb{G}) \cong \text{ a subgroup of a cyclic group of order } m$$

and we see that $\tau(g) = 1$ for all g if $\mathbb{G}$ contains no non-trivial cyclic quotient group of order dividing m. □

3.3.3 Note The following example shows that the relevant hypothesis cannot be disposed of altogether. Let $\mathbb{H} = \langle i, j \mid i^4 = 1, j^2 = i^2, jij^{-1} = i^{-1}\rangle$ and let $\mathbb{G}$ be the subgroup

of $\mathrm{Aut}(\mathbb{H})$ generated by $\{a, z\}$, where a is conjugation by ij and z is the automorphism that swaps i and j. Then $\mathbb{G}$ is the Klein group of four elements and z is central in $\mathbb{G}$. Let $\mathbf{S}$ be the two-dimensional complex representation of $\mathbb{H}$ defined by

$$i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad j = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$$

This is $\mathbb{G}$-invariant and can be extended to $\mathbb{H} \rtimes \langle z \rangle$ in precisely two ways:

$$z = \pm \frac{1}{\sqrt{-2}} \begin{pmatrix} \sqrt{-1} & 1 \\ -1 & -\sqrt{-1} \end{pmatrix}$$

with characters $\pm\phi$. However, $\mathrm{tr}(z) = 0$ and $(\pm\phi)^a = \mp\phi$. Thus, none of $\pm\phi$ is $\mathbb{G}$-invariant, and therefore $\mathbf{S}$ cannot be extended to an ordinary representation of $\mathbb{H} \rtimes \mathbb{G}$.

3.4 Hilbert's Theorem 90 for matrices

The results contained in this section are all known. They are required in the computation of the Schur index of the Weil representation and are included for the sake of completeness. Part of the presentation is extracted from (unpublished) notes written by Mazi Shirvani.

Let $\mathbb{K} \subseteq \mathbb{F}$ be a finite separable field extension and let $\mathfrak{S}$ be a set of $n \times n$ matrices with coefficients in $\mathbb{F}$. We are interested in the following:

When and how is $\mathfrak{S}$ realizable over $\mathbb{K}$? That is, under which conditions there exists $A \in \mathrm{GL}_d(\mathbb{F})$ such that $ASA^{-1} \in \mathrm{M}_n(\mathbb{K})$ for all $S \in \mathfrak{S}$?

We are mainly interested in the case when $\mathfrak{S} = T(G)$ and $T : G \to \mathrm{GL}_d(\mathbb{F})$ is an absolutely irreducible representation of a group G all whose character values are contained in $\mathbb{K}$.

Note that there is no loss of generality in supposing that $\mathbb{K} \subseteq \mathbb{F}$ is a finite Galois extension with Galois group Gal, and we shall make this assumption. Accordingly, a matrix $A \in \mathrm{GL}_d(\mathbb{F})$ realizes $\mathfrak{S}$ over $\mathbb{K}$ if and only if

$$^{\sigma}(ASA^{-1}) = ASA^{-1},$$

that is

$$^{\sigma}S = (^{\sigma}A)^{-1}AS((^{\sigma}A)^{-1}A)^{-1}$$

for all $\sigma \in \mathrm{Gal}$ and $S \in \mathfrak{S}$. Thus if $\mathfrak{S}$ is realizable over $\mathbb{K}$, there exists $L_\sigma = ({}^\sigma A)^{-1} A \in \mathrm{GL}_d(\mathbb{F})$ such that

$$ {}^\sigma S = L_\sigma S L_\sigma^{-1} \tag{3.25}$$

for all $S \in \mathfrak{S}$ and $\sigma \in \mathrm{Gal}$.

In order to make progress we shall assume henceforth that $\mathfrak{S}$ is equivalent to its Galois conjugates; that is, there exist $(L_\sigma)_{\sigma \in \mathrm{Gal}}$ in $\mathrm{GL}_d(\mathbb{F})$ such that (3.25) holds. Furthermore, we shall assume that the centralizer of $\mathfrak{S}$ in $\mathrm{M}_d(\mathbb{F})$ is equal to $\mathbb{F}.1_d$. Under these hypothesis the above discussion translates into

3.4.1 Proposition $A \in \mathrm{GL}_d(\mathbb{F})$ realizes $\mathfrak{S}$ over $\mathbb{K}$ if and only if there exist $(\alpha_\sigma)_{\sigma \in \mathrm{Gal}}$ in $\mathbb{F}^*$ such that

$$ ({}^\sigma A)^{-1} A = \alpha_\sigma L_\sigma \tag{3.26}$$

for all $\sigma \in \mathrm{Gal}$.

Applying $\tau \in \mathrm{Gal}$ to (3.25) and comparing the result with the corresponding expression for $\tau\sigma$ (this means apply σ first, then τ) we deduce the existence of $f(\tau, \sigma) \in \mathbb{F}^*$ satisfying

$$ L_{\tau\sigma} = f(\tau, \sigma)^\tau L_\sigma L_\tau. \tag{3.27}$$

The associative law of Gal implies that $f \in Z^2(\mathrm{Gal}, \mathbb{F}^*)$, that is

$$ {}^\tau f(\sigma, \theta) f(\tau, \sigma\theta) = f(\tau\sigma, \theta) f(\tau, \sigma) $$

and we see that f changes by a coboundary when L_σ is replaced by a scalar multiple. This gives a uniquely determined element $[f] \in H^2(\mathrm{Gal}, \mathbb{F}^*)$.

Suppose that A realizes $\mathfrak{S}$ over $\mathbb{K}$, so that $L_\sigma = \alpha_\sigma^{-1} ({}^\sigma A)^{-1} A$. Substituting this into (3.27) we get

$$ f(\tau, \sigma) = {}^\tau \alpha_\sigma \alpha_{\tau\sigma}^{-1} \alpha_\tau, \tag{3.28}$$

that is $[f] = 1$.

3.4.2 Proposition A necessary condition for the realizability of $\mathfrak{S}$ over $\mathbf{K}$ is that $[f] = 1$.

Suppose, conversely, that (3.28) holds. Then setting $M_\sigma = \alpha_\sigma L_\sigma$ we obtain

$$M_{\tau\sigma} = {}^{\tau}M_\sigma M_\tau,$$

which means that $M \in H^1(\mathrm{Gal}, \mathrm{GL}_d(\mathbf{F}))$. But this set is trivial ([Ser79], Section X.1, Proposition 3), which means that there exists $A \in \mathrm{GL}_d(\mathbf{F})$ such that $({}^{\sigma}A)^{-1}A = M_\sigma = \alpha_\sigma L_\sigma$.

3.4.3 Proposition A sufficient condition for the realizability of $\mathfrak{S}$ over $\mathbf{K}$ is that $[f] = 1$.

Given $\sigma \in \mathrm{Gal}$ denote by r the order of σ and by $\mathbf{F}^\sigma$ the fixed field of σ. Observe that

$$\begin{aligned} S = L_\sigma^{-1} \cdot {}^{\sigma}S \cdot L_\sigma &= (L_\sigma)^{-1} \cdot ({}^{\sigma}L_\sigma)^{-1} \cdot {}^{\sigma^2}S \cdot {}^{\sigma}L_\sigma \cdot L_\sigma = \ldots \\ &= \left({}^{\sigma^{(r-1)}}L_\sigma \ldots {}^{\sigma}L_\sigma L_\sigma\right)^{-1} S^{\sigma^{(r-1)}} L_\sigma \ldots {}^{\sigma}L_\sigma L_\sigma \end{aligned}$$

and therefore

$${}^{\sigma^{(r-1)}}L_\sigma \ldots {}^{\sigma}L_\sigma L_\sigma = a_\sigma \tag{3.29}$$

is a non-zero scalar in $\mathbf{F}$. Applying σ to (3.29) and noting that L_σ commutes with ${}^{\sigma^{(r-1)}}L_\sigma \ldots {}^{\sigma}L_\sigma$ (their product is a scalar) we see that a_σ actually belongs to $\mathbf{F}^\sigma$.

If A realizes $\mathfrak{S}$ over $\mathbf{K}$ then (3.26) gives

$$\begin{aligned} A = \alpha_\sigma \cdot {}^{\sigma}A \cdot L_\sigma &= \alpha_\sigma \cdot {}^{\sigma}\alpha_\sigma \cdot {}^{\sigma^2}A \cdot {}^{\sigma}L_\sigma \cdot L_\sigma = \ldots \\ &= \alpha_\sigma {}^{\sigma}\alpha_\sigma \ldots {}^{\sigma^{(r-1)}}\alpha_\sigma \cdot A \cdot {}^{\sigma^{(r-1)}}L_\sigma \ldots {}^{\sigma}L_\sigma L_\sigma. \end{aligned}$$

Thus, (3.29) yields

$$\alpha_\sigma {}^{\sigma}\alpha_\sigma \ldots {}^{\sigma^{(r-1)}}\alpha_\sigma = a_\sigma^{-1},$$

whence

$$N_{\mathbf{F}/\mathbf{F}^\sigma}(\alpha_\sigma) = a_\sigma^{-1}.$$

3.4.4 Proposition A necessary condition for the realizability of $\mathfrak{S}$ over $\mathbf{K}$ is the solvability of the norm equations $N_{\mathbf{F}/\mathbf{F}^\sigma}(x) = a_\sigma^{-1}$, $\sigma \in \mathrm{Gal}$.

In order to analize the sufficiency of this condition we make the further assumption that Gal is solvable. Accordingly, let $1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_m = \mathrm{Gal}$ be a subnormal series for Gal, where G_{i+1}/G_i is cyclic. Then $\mathbf{F} = F^{G_0} \supseteq \mathbf{F}^{G_1} \supseteq \ldots \supseteq \mathbf{F}^{G_m} = \mathbf{K}$ is a descending chain of sub-extensions of $\mathbf{F}/\mathbf{K}$, where $\mathbf{F}^{G_i}/\mathbf{F}^{G_{i+1}}$ is Galois with Galois group G_{i+1}/G_i. Since $\mathfrak{S}$ is realizable over $\mathbf{K}$ if and only if $\mathfrak{S}$ is realizable over $\mathbf{F}^{G_i}$ for all i, there is no harm, *in theory*, in assuming that $\mathbf{F}/\mathbf{K}$ is cyclic with Galois group $\mathrm{Gal} = \langle\sigma\rangle$ of order r.

Set $L = L_\sigma$ and $a = a_\sigma$. Make the (valid) choice

$$L_{\sigma^i} = {}^{\sigma^{i-1}}L \cdots {}^{\sigma}LL, \quad 0 \leq i < r.$$

According to this choice, we have

$$f(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j < r \\ a & \text{otherwise} \end{cases}$$

for all $0 \leq i, j < r$. Suppose that $N_{\mathbf{F}/\mathbf{K}}(\alpha) = a^{-1}$ for some $\alpha \in \mathbf{K}^*$. Then, if we set

$$\beta_{\sigma^i} = \alpha^\sigma \alpha \cdots {}^{\sigma^{(r-1)}}\alpha$$

and

$$\alpha_{\sigma^i} = (\beta_{\sigma^i})^{-1}$$

for all $0 \leq i < r$, we see that (3.28) holds for all elements of Gal.

3.4.5 Proposition If Gal is cyclic then a sufficient condition for the realizability of $\mathfrak{S}$ over $\mathbf{K}$ is the solvability of the norm equation $N_{\mathbf{F}/\mathbf{K}}(x) = a^{-1}$.

As a corollary we obtain

3.4.6 Proposition Let $\mathbf{K} \subseteq \mathbf{F}$ be a finite cyclic Galois extension with Galois group $\langle\sigma\rangle$ of order r. Let $T : G \to \mathrm{GL}_d(\mathbf{F})$ be an absolutely irreducible matrix representation of

an arbitrary group G, and let the character ϕ of T have values in $\mathbf{K}$. Let $L \in \mathrm{GL}_d(\mathbf{F})$ be the unique -up to scaling- operator satisfying

$$LT(g)L^{-1} = {}^{\sigma}T(g)$$

for all $g \in G$ (such an L exists because ${}^{\sigma}\phi = \phi$). Then ${}^{\sigma^{r-1}}L \cdots {}^{\sigma}LL = a$ is a non-zero scalar in $\mathbf{K}$ and T is realizable over $\mathbf{K}$ if and only if the norm equation $N_{\mathbf{F}/\mathbf{K}}(x) = a^{-1}$ is solvable.

The name of this section derives from the ensuing result, whose proof is contained in the preceding discussion.

3.4.7 Proposition Let $\mathbf{K} \subseteq \mathbf{F}$ be a finite cyclic Galois extension with Galois group $\langle\sigma\rangle$ of order r. Then $L \in \mathrm{GL}_d(\mathbf{K})$ satisfies

$${}^{\sigma^{r-1}}L \cdots {}^{\sigma}LL = 1_d$$

if and only if

$$L = ({}^{\sigma}A)^{-1}A$$

for some $A \in \mathrm{GL}_d(\mathbf{K})$.

Chapter 4

The Schrödinger and Weil Representations

Denote by H the Heisenberg group associated to the symplectic space $(V, \langle\ ,\ \rangle)$; that is

$$H = H(R, V, \langle\ ,\ \rangle) = H_{2n}(R) = \{(r, v) : r \in R, v \in V\}$$

with multiplication given by

$$(r, v)(r', v') = (r + r' + \langle v, v' \rangle, v + v').$$

Then

$$(r, v)^{-1} = (-r, -v), \quad {}^{(s,w)}(r, v) = (r + 2\langle w, v \rangle, v)$$

and

$$Z(H) = (R, 0) = H'.$$

Note that GSp acts on H by means of

$${}^{g}(r, v) = (k(g)r, gv). \tag{4.1}$$

Assume henceforth that R admits an additive primitive linear character λ. In view of Proposition 3.2.3 this is equivalent to saying that each local component of R is an irreducible ring. Under this assumption there exists a unique irreducible character η of

H whose restriction to $Z(H)$ is a multiple of λ. In view of the action (4.1) of Sp on H, η must be Sp-invariant; a Weil representation of Sp is one that intertwines the Sp-conjugates of a given S affording η. We proceed to prove the existence of these truly fascinating representations.

4.1 The existence of the Schrödinger Representation and its consequences

4.1.1 Lemma Let $E \lhd G$ be finite groups and ϕ, χ absolutely irreducible characters of E and G respectively. Suppose that $\chi|_E = d\phi$ for some positive integer d. Then χ is the only irreducible character of G lying over ϕ if and only if $d^2 = [G : E]$.

Proof: $\Rightarrow$ By Frobenius reciprocity and hypothesis $\mathrm{ind}_E^G\phi = d\chi$. Thus

$$d^2 = [\mathrm{ind}_E^G\phi, \mathrm{ind}_E^G\phi] = [\phi, \mathrm{res}_E^G\mathrm{ind}_E^G\phi] = [\phi, [G : E]\phi] = [G : E],$$

since ϕ is G-invariant. $\Leftarrow$ By Frobenius reciprocity χ enters d times in $\mathrm{ind}_E^G\phi$. On the other hand, since $\chi|_E = d\phi$ and $d^2 = [G : E]$

$$\deg d\chi = d^2 \deg\phi = \deg \mathrm{ind}_E^G\phi,$$

whence $\mathrm{ind}_E^G\phi = d\chi$. By Frobenius reciprocity no irreducible character of G other than χ lies over ϕ. □

Given a submodule L of V denote by $\hat{L}$ the group of all complex linear characters of L. If $v \in V$ denote by l_v the element of $\hat{V}$ defined by

$$l_v(u) = \lambda(2\langle v, u\rangle), \quad u \in V.$$

4.1.2 Lemma If L is a submodule of V then the map

$$V \ni v \to l_v|_L \in \hat{L} \tag{4.2}$$

is a group homomorphism with kernel $L^\perp$.

Proof: It is clear that (4.2) is a group homomorphism. Suppose that v belongs to its kernel. Since L is a submodule and 2 is invertible in R the set

$$I_{v,L} = \{\langle v, u\rangle \mid u \in L\} = \{2\langle v, u\rangle \mid u \in L\}$$

is an ideal of R contained in the kernel of λ. Given the primitivity of λ we have $I_{v,L} = (0)$ and, a fortiori, $v \in L^{\perp}$. □

4.1.3 Corollary Let L be a totally isotropic submodule of V and ρ any extension of λ to (R, L). Then the inertia group of ρ in H is equal to $(R, L^{\perp})$.

Proof:

$$\begin{aligned}(r, v) \in \mathrm{Stab}_H(\rho) &\Leftrightarrow \rho^{(r,v)}(s, u) = \rho(s, u), \quad s \in R, u \in L \\ &\Leftrightarrow \rho(s + 2\langle v, u\rangle, u) = \rho(s, u), \quad s \in R, u \in L \\ &\Leftrightarrow \lambda(2\langle v, u\rangle) = 1, \quad u \in L \\ &\Leftrightarrow v \in L^{\perp}.\end{aligned}$$

□

In the sequel we shall denote by ρ_0 the extension of λ to (R, L) that is trivial on L. The next fundamental result was proven in collaboration with Gerald Cliff and David A. McNeilly.

4.1.4 Theorem Let $A = (R, M)$ and set $\eta = \eta_\lambda = \mathrm{ind}_A^H \rho_0$. Then η is an absolutely irreducible character of H of degree $|R|^n$ whose restriction to $Z(H)$ is equal to $|R|^n\lambda$.

Proof: The inertia group of ρ_0 in H is precisely A, due to Corollary 4.1.3. By Clifford theory η is absolutely irreducible and moreover

$$\eta|_{Z(H)} = [H : A]\lambda = [V : M]\lambda = |R|^n\lambda.$$

□

We shall refer to η_λ as the Schrödinger character of H associated to λ, and any representation $S = S_\lambda$ affording it will be called the Schrödinger representation of H associated to λ. The Schrödinger module will be denoted by X.

The rest of this section is devoted to study the numerous consequences of Theorem 4.1.4. The first of these says that η_λ is bound to λ by a very strong relationship. Indeed, the number of times that λ appears in $\eta_\lambda|_{Z(H)}$ is equal to the square root of $[H : Z(H)]$, hence Lemma 4.1.1 gives

4.1.5 Corollary η_λ is the unique irreducible character of H whose restriction to $Z(H)$ is a multiple of λ.

Accordingly, there is great freedom in the way η_λ can be constructed from λ.

4.1.6 Corollary Let L be a totally isotropic submodule of V and ρ any extension of λ to $A = (R, L)$. Then $\mathrm{ind}_A^H \rho$ is a multiple of η_λ. It is equal to η_λ if and only if $L \in \mathcal{M}$.

Proof: The restriction of $\mathrm{ind}_A^H \rho$ to $Z(H)$ is a multiple of λ and Corollary 4.1.5 applies. This proves the first assertion. According to Corollary 4.1.3 $\mathrm{ind}_A^H \rho$ is irreducible if and only if $L \in \mathcal{M}$, as required in the second assertion. □

The fact that so many different paths lead to the same object has strong consequences.

4.1.7 Corollary If L is a totally isotropic submodule of V then the map (4.2) is an epimorphism. Thus all extensions of λ to $A = (R, L)$ are H-conjugate to one another.

Proof: Let $\phi \in \hat{L}$ and define the extension ρ of λ to A by means of

$$\rho(s, u) = \lambda(s)\phi(u), \quad s \in R, u \in L.$$

By Corollary 4.1.6 η enters both $\mathrm{ind}_A^H \rho$ and $\mathrm{ind}_A^H \rho_0$. By Frobenius reciprocity both ρ and ρ_0 enter $\eta|_A$. But by Clifford theory all components of $\eta|_A$ are H-conjugate. Thus there exists $(r, v) \in H$ such that $\rho = \rho_0^{(r,v)}$; that is

$$\lambda(s)\phi(u) = \rho(s, u) = \rho_0^{(r,v)}(s, u) = \rho_0(s + 2\langle v, u\rangle, u) = \lambda(s)\lambda(2\langle v, u\rangle)$$

for all $s \in R, u \in L$. We conclude that

$$\phi = l_v|_L,$$

as desired. □

Denote by $\mathcal{A}$ the collection of all maximal abelian subgroups A of H. Note that any such A must necessarily contain $Z(H)$ and it is therefore normal in H. We easily see that

$$\mathcal{M} \ni L \leftrightarrow (R, L) = A \in \mathcal{A}$$

establishes a bijection between $\mathcal{M}$ and $\mathcal{A}$.

4.1.8 Corollary Let $A = (R, L) \in \mathcal{A}$. Then $\eta|_A$ is the sum of all extensions of λ to A.

Proof: Since $\mathrm{Stab}_H \rho_0 = A$, $\eta|_A$ is the sum of all H-conjugates of ρ_0, with no repetitions. In light of Corollary 4.1.7 every extension of λ to A is H-conjugate to ρ_0, as desired. □

4.1.9 Corollary Let L be a totally isotropic submodule of V. Then

$$|L||L^{\perp}| = |V|. \tag{4.3}$$

Thus

$$|L||L^{0}| = |V| \tag{4.4}$$

and

$$L \in \mathcal{M} \Leftrightarrow |L|^2 = |V| \Leftrightarrow |L| = |R|^n. \tag{4.5}$$

Proof: In view of Lemma 4.1.2 and Corollary 4.1.7 we have

$$|L||L^{\perp}| = |\hat{L}||L^{\perp}| = |V|.$$

This implies (4.4) in virtue of the equality $|L^{\perp}| = |L^{0}|$. Likewise, (4.5) follows from (4.3) and $L \subseteq L^{\perp}$. □

We are in a position to prove the following amazing result:

4.1.10 Theorem Let R be a finite commutative ring of odd characteristic. Then the following conditions are equivalent:

(a) Each local component of R is irreducible.

(b) R possesses a primitive linear character.

(c) $\mathrm{Ann}(\mathrm{Ann}(I)) = I$ for any ideal I of R.

(d) $|I||\mathrm{Ann}(I)| = |R|$ for any ideal I of R.

(e) If $\mathbf{V}$ is free R-module of finite rank and $\mathbf{L}$ is a submodule of $\mathbf{V}$ then $|\mathbf{L}||\mathbf{L}^0| = |\mathbf{V}|$.

(f) If $\mathbf{V}$ is free R-module of finite rank and $\mathbf{L}$ is a submodule of $\mathbf{V}$ then ${}^0(\mathbf{L}^0) = \mathbf{L}$.

Here ${}^0(\mathbf{L}^0)$ denotes the set of zeros of $\mathbf{L}^0$.

Proof: (a)$\Leftrightarrow$(b) Proposition 3.2.3. (b)$\Rightarrow$(e),(f) Set $\mathbf{V}_0 = \mathbf{V} \oplus \mathbf{V}$ and endow $\mathbf{V}_0$ with a non-degenerate alternating form that makes $\mathbf{V}$ a maximal totally isotropic subspace. Write $\mathbf{L}_0$ for $\mathbf{L}$ considered as a subspace of $\mathbf{V}_0$. Corollary 4.1.9 applies, yielding

$$|\mathbf{L}_0||\mathbf{L}_0^0| = |\mathbf{V}_0|.$$

But we easily see that

$$|\mathbf{L}_0^0| = |\mathbf{L}^0||\mathbf{V}|,$$

whence (e) follows. We can now obtain (f) as a formal consequence of (e). Indeed, applying (e) to $\mathbf{L}^0$ we get

$$|\mathbf{L}^0||\mathbf{L}^{00}| = |\mathbf{V}^*| = |\mathbf{V}|.$$

Making use of the natural isomorphism $\mathbf{V} \to \mathbf{V}^{**}$ we obtain

$$|\mathbf{L}^0||{}^0(\mathbf{L}^0)| = |\mathbf{V}|. \tag{4.6}$$

But $\mathbf{L} \subseteq {}^0(\mathbf{L}^0)$, hence (e) and (4.6) give (f). (e)$\Rightarrow$(c) Let $\mathbf{V}$ be R. (f)$\Rightarrow$(d) Let $\mathbf{V}$ be R. (c)$\Rightarrow$(a) We can safely assume that R is local and then take I to be any minimal ideal. (d)$\Rightarrow$(a) We can safely assume that R is local and then take $I = \mathfrak{m}$. □

4.2 The Weil Representation and its ordinary nature

4.2.1 Definition A representation $W = W_\lambda : \mathrm{Sp} \to \mathrm{GL}(X)$ satisfying

$$W(g)S(h)W(g)^{-1} = S({}^g h) \tag{4.7}$$

for all $g \in \mathrm{Sp}$, $h \in H$, will be referred to as a Weil representation of Sp associated to λ. Its character will be denoted by $\Omega = \Omega_\lambda$.

The aim of this section is to prove the existence of this wonderful representation. We start by showing that η_λ is indeed Sp-invariant. More generally, we describe the behavior of the Schrödinger character when subjected to the action of objects outside H.

4.2.2 Corollary The Schrödinger characters of H are GSp-conjugates. In fact, for any $g \in \mathrm{GSp}$ we have

$$\eta_\lambda^g = \eta_{\lambda[k(g)]}$$

Proof: Immediate consequence of Lemma 3.2.4 and Corollary 4.1.5. □

The next corollary was obtained in collaboration with Gerald Cliff and David A. McNeilly.

4.2.3 Corollary η_λ is Sp-invariant.

This ensures the existence of a projective representation P of Sp satisfying

$$P(g)S(h)P(g)^{-1} = S({}^g h), \quad g \in \mathrm{Sp},\ h \in H. \tag{4.8}$$

Finally, we show that the Schrödinger characters $\eta_{\lambda[k]}$, $k \in (\mathbf{Z}/c\mathbf{Z})^* \subseteq R^*$, form a Galois-orbit. Indeed, consider the isomorphism

$$(\mathbf{Z}/c\mathbf{Z})^* \ni k \to \sigma(k) \in \mathrm{Gal}(F, \mathbf{Q}),$$

where $\sigma(k)$ is the automorphism $\zeta_c \mapsto \zeta_c^k$. We can thus subject η_λ to the action of $\sigma(k)$ and apply Corollary 4.1.5 to obtain

4.2.4 Corollary For any $k \in (\mathbf{Z}/c\mathbf{Z})^*$ we have

$${}^{\sigma(k)}\eta_\lambda = \eta_{\sigma(k)\lambda} = \eta_{\lambda[k]}.$$

We next produce a Schrödinger module X_L for each $L \in \mathcal{M}$ and construct a map $P_L : \mathrm{Sp}_L \to \mathrm{GL}(X)$ that satisfies (4.8) and is also a group homomorphism from the subgroup Sp_L of Sp that preserves L. This requires the use of new notation, to be used extensively in what follows.

The symbol $\mathcal{T}$ will be reserved to designate a transversal. We shall usually feel the need to be quite specific about transversals; thus, if V_0 is a submodule of V then by $\mathcal{T}(V/V_0)$ we shall mean a transversal of V relative to V_0. We can always choose $\mathcal{T}(V/V_0)$ so that it is -1-invariant, and this will be the only type of transversal of V ever to be considered. Note that $0 \in \mathcal{T}(V/V_0)$. By $\mathcal{S}(V/V_0)$ we shall understand a subset of $\mathcal{T}(V/V_0)\setminus\{0\}$ that contains precisely one element out of every pair $\{v,-v\}$ of non-zero elements of $\mathcal{T}(V/V_0)$; We shall refer to $\mathcal{S}(V/V_0)$ as a moiety of $\mathcal{T}(V/V_0)\setminus\{0\}$. Note that $|\mathcal{S}(V/V_0)| = (|\mathcal{T}(V/V_0)|-1)/2$.

Given $A=(R,L)\in\mathcal{A}$, extend λ to linear character ρ of $A\rtimes \mathrm{Sp}_L$ as follows:

$$\rho((r,u)g)=\lambda(r),\quad r\in R,\ u\in L,\ g\in \mathrm{Sp}_L.$$

Let $A\rtimes \mathrm{Sp}_L\to \mathrm{GL}(Y)$ be a one-dimensional representation affording ρ; that is $Y=Fy$ and

$$(r,u)g\cdot y=\lambda(r)y,\quad r\in R,\ u\in L,\ g\in \mathrm{Sp}_L.$$

Consider the induced character

$$\phi_L=\mathrm{ind}_{A\rtimes \mathrm{Sp}_L}^{H\rtimes \mathrm{Sp}_L}\rho$$

afforded by the induced module

$$X_L=\mathrm{ind}_{A\rtimes \mathrm{Sp}_L}^{H\rtimes \mathrm{Sp}_L}Y=F(H\rtimes \mathrm{Sp}_L)\otimes_{F(A\rtimes \mathrm{Sp}_L)}Y.$$

This gives a representation

$$H\rtimes \mathrm{Sp}_L\to \mathrm{GL}(X_L) \tag{4.9}$$

whose restriction to Sp_L we denote by P_L. We are ready to state

4.2.5 Lemma Given $L\in\mathcal{M}$, write $X=X_L$ and $P=P_L$. Then

(a) The restriction of (4.9) to H is the Schrödinger representation S of H associated to λ.

(b) Let $\mathcal{T}=\mathcal{T}(V/L)$ and

$$e_v=(0,v)\otimes y,\quad v\in\mathcal{T}.$$

Then $(e_v)_{v\in\mathcal{T}}$ is an F-basis of X.

(c) P satisfies (4.8) and its action on X is given by

$$P(g)e_v = \lambda(\langle gv, v'\rangle)e_{v'}. \tag{4.10}$$

Here $g \in \mathrm{Sp}_L$, v runs through $\mathcal{T}$ and $v' \in \mathcal{T}$ satisfies $gv \equiv v' \mod L$.

(d)

$$P(\iota)e_v = e_{-v}, \quad v \in \mathcal{T}. \tag{4.11}$$

(e)

$$\mathrm{tr}(P(\iota)) = 1. \tag{4.12}$$

(f) The ± 1-eigenspaces $X_\pm$ of $P(\iota)$ have dimensions

$$(|R|^n + 1)/2 \text{ and } (|R|^n - 1)/2.$$

(g) If $\mathcal{S} = \mathcal{S}(V/L)$ then $X_\pm$ have bases

$$(e_0, (e_v + e_{-v})_{v\in\mathcal{S}}) \text{ and } (e_v - e_{-v})_{v\in\mathcal{S}}.$$

(h)

$$(\det P(\iota)|_{X_+})^{-1}(\det P(\iota)|_{X_-}) = (-1)^{(|R|^n-1)/2} = \mu(-1)^n. \tag{4.13}$$

Proof: (a) The restriction of ϕ_L to $Z(H)$ equals $|R|^n\lambda$ and Corollary 4.1.5 applies. (b) $\mathcal{T}$ is a transversal of H relative to A and hence of $H \rtimes \mathrm{Sp}_L$ relative to $A \rtimes \mathrm{Sp}_L$. Since Y is one-dimensional, the result follows from abstract nonsense. (c) Since (4.9) is a group homomorphism whose restriction to H is the Schrödinger representation, it must satisfy (4.8) when restricted to Sp_L. This proves the first assertion. As for the second, if $gv = v' + u$, $u \in L$, then

$$\begin{aligned} ge_v &= g(0,v)\otimes y = {}^g(0,v)g\otimes y = (0,gv)\otimes gy = (0,v'+u)\otimes y \\ &= (0,v')\otimes(\langle u,v'\rangle,0)(0,u)y = \lambda(\langle gv,v'\rangle)e_{v'}. \end{aligned}$$

(d) Make the substitution $g = \iota$ in (4.10). (e) Immediate consequence of (d). (f) Immediate consequence of (e) and $P(\iota)^2 = 1_X$. (g) Immediate consequence of (b) and (d). (h) The very definitions of X_+ and X_- in conjunction with (f) give

$$(\det P(\iota)|_{X_+})^{-1}(\det P(\iota)|_{X_-}) = (1)^{(|R|^n+1)/2}(-1)^{(|R|^n-1)/2} = (-1)^{(|R|^n-1)/2}$$
$$= (-1)^{\frac{n(|R|-1)}{2}}.$$

On the other hand the very definition of μ gives

$$\mu(-1) = (-1)^{\frac{(|R|-1)}{2}}.$$

Thus

$$\mu(-1)^n = (-1)^{\frac{n(|R|-1)}{2}} = (\det P(\iota)|_{X_+})^{-1}(\det P(\iota)|_{X_-}).$$

□

A projective representation P of Sp satisfying (4.8) will be said to be normalized if $P(\iota)$ has trace equal to 1. Note that that if P and P' are normalized then $P'(\iota) = P(\iota)$. Indeed, since S is absolutely irreducible, $P'(\iota) = aP(\iota)$ for some $a \in F$, whence $a = 1$ by taking traces. As a consequence of Lemma 4.2.5 and Propositions 3.3.1 and 3.3.2 applied to $z = \iota$ we obtain

4.2.6 Theorem A Weil representation W of Sp exists. In fact, let P any normalized projective representation satisfying (4.8) and let $X_\pm$ be the ± 1-eigenspaces of $P(\iota)$. Further, set $c(g) = (\det P(g)|_{X_+})^{-1}(\det P(g)|_{X_-})$. Then $W(g) = P(g)c(g)$ defines an ordinary representation of Sp satisfying (4.7).

4.3 Reduction to the local case

It seems appropriate at this point to show how one can restrict the theory to the local case. Write $R = R_1 \times ... \times R_t$, a direct product of local rings. Then

$$\lambda(r_1, ..., r_t) = \lambda_1(r_1)...\lambda_t(r_t)$$

where λ_i is a primitive linear character of R_i. Let $S_{\lambda_i} : H_{2n}(R_i) \to \mathrm{GL}(X_i)$ be the Schrödinger representation associated to λ_i and let $W_{\lambda_i} : \mathrm{Sp}_{2n}(R_i) \to \mathrm{GL}(X_i)$ be a Weil

representation associated to λ_i. For each j set $I_j = \prod_{i \neq j} R_i$ and use the notation that preceeds (2.27).

4.3.1 Proposition The natural map

$$H_{2n}(R) \ni h \mapsto (h_{I_1}, ..., h_{I_t}) \in H_{2n}(R_1) \times ... \times H_{2n}(R_t)$$

is a group isomorphism compatible with (2.28), in the sense that

$$(({}^g h)_{I_1}, ..., ({}^g h)_{I_t}) = ({}^{g_{I_1}} h_{I_1}, ..., {}^{g_{I_t}} h_{I_t}).$$

Thus

$$H_{2n}(R) \ni h \mapsto S_{\lambda_1}(h_{I_1}) \otimes ... \otimes S_{\lambda_t}(h_{I_t}) \in \mathrm{GL}(X_1 \otimes ... \otimes X_t)$$

is the Schrödinger representation associated to λ and

$$\mathrm{Sp}_{2n}(R) \ni g \mapsto W_{\lambda_1}(g_{I_1}) \otimes ... \otimes W_{\lambda_t}(g_{I_t}) \in \mathrm{GL}(X_1 \otimes ... \otimes X_t)$$

is a Weil representation associated to λ.

Proof: It all follows from the very definitions of the objects involved.

4.4 Uniqueness of the Weil Representation

Assume here that R is an irreducible ring.

4.4.1 Lemma Sp possesses a unique Weil representation of associated to λ, provided $n \neq 1$ or $q \neq 3$.

Proof: Suppose that W and W' satisfy (4.7). Given the absolute irreducibility of S, $W = \tau W'$, for some linear character τ of Sp. If $n \neq 1$ or $q \neq 3$ then Sp is perfect (Corollary 2.4.4), whence $\tau = 1$ and, a fortiori, $W' = W$. □

We shall shortly distinguish amongst the Weil representations arising in the imperfect case. In the meantime, we shall speak freely of *the* Weil representation whenever we deem it convenient.

Chapter 5

Construction of the Weil Representation

We shall merely assume here that R admits an additive primitive linear character λ. There will be no need to make use of the structure of local rings.

In this chapter we construct a Weil representation $W = W_\lambda$ following the procedure indicated in Theorem 4.2.6. We shall assume to start off that $X = X_M$ and P is any projective representation of Sp that satisfies (4.8) and extends P_M. Let $\mathcal{T} = \mathcal{T}(V/M) = N$ and denote by $\mathcal{S}$ a moiety of $N \setminus \{0\}$. Then

$$(e_0, (e_v + e_{-v})_{v\in\mathcal{S}}) \quad \text{and} \quad (e_v - e_{-v})_{v\in\mathcal{S}} \tag{5.1}$$

are F-bases for the ± 1-eigenspaces X_+ and X_- of $P(\iota)$, and

$$c(g) = (\det P(g)|_{X_+})^{-1}(\det P(g)|_{X_-}) \tag{5.2}$$

for each $g \in \mathrm{Sp}$. Since $W|_{\mathrm{Sp}_M}$ and P_M are group homomorphisms, so must be the correcting factor $c|_{\mathrm{Sp}_M} : \mathrm{Sp}_M \to F^*$.

We shall define W on the generators of Sp given in Corollary 2.3.7. For reasons that will become apparent in Section 5.7 we want to define W on all $g^N(r)$, $r \in R$. In order to achieve our goal we shall

(a) Compute $c(g)$ for each $g \in \mathrm{Sp}^M$.

(b) Compute $c(g)$ for each $g \in \mathrm{Sp}_{M,N}$.

(c) Find a $P(g) \in \mathrm{GL}(X)$ satisfying (4.8) for each $g \in \mathrm{Sp}^N$.

(d) Compute $c(g)$ for each $g \in \mathrm{Sp}^N$.

We proceed to carry out this program

5.1 Construction of W on Sp^M

Let $g \in \mathrm{Sp}^M$ and $v \in N$. Then the translation of (4.10) into our setting reads

$$P(g)e_v = \lambda(\langle gv, v\rangle)e_v. \tag{5.3}$$

We have used the fact that $gv - v \in M$ (Lemma 2.3.2(a)). Thus

$$P(g)(e_v \pm e_{-v}) = \lambda(\langle gv, v\rangle)(e_v \pm e_{-v})$$

for all $v \in \mathcal{S}$, whereby

$$c(g) = \lambda(\langle g0, 0\rangle)^{-1} = 1.$$

We have thus established the following equations:

$$W(g)e_v = \lambda(\langle gv, v\rangle)e_v, \tag{5.4}$$

$$\Omega(g) = \sum_{v \in N} \lambda(\langle gv, v\rangle). \tag{5.5}$$

In particular, if g is the symplectic transvection ρ_{r,u_1} then

$$\Omega(g) = |R|^{n-1} \sum_{s \in R} \lambda(rs^2). \tag{5.6}$$

Indeed, we have $gv = v + r\langle u_1, v\rangle u_1$, whence $\langle gv, v\rangle = r\langle u_1, v\rangle^2$. Thus (5.5) gives

$$\Omega(g) = \sum_{s_1,\ldots,s_n \in R} \lambda(r\langle u_1, s_1v_1 + \ldots + s_nv_n\rangle^2) = |R|^{n-1} \sum_{s_1 \in R} \lambda(rs_1^2).$$

5.2 Construction of W on $\mathrm{Sp}_{M,N}$

Let $g \in \mathrm{Sp}_{M,N}$ and $v \in N$. Then (4.10) gives

$$P(g)e_v = e_{gv}, \tag{5.7}$$

since gv also belongs to N. The definition (5.2) thus yields the group homomorphism $c|_{\mathrm{Sp}_{M,N}}$, defined by

$$g \ni \mathrm{Sp}_{M,N} \mapsto (-1)^{|\{v \in \mathcal{S} \mid gv \in -\mathcal{S}\}|} \in \{\pm 1\},$$

which is nothing but $\mu(\mathrm{Sp}_{M,N}, N \setminus \{0\})$. In view of (3.3) and the identification (2.8), we have

$$c|_{\mathrm{Sp}_{M,N}}(g) = \mu(\det g|_N)$$

for all $g \in \mathrm{Sp}_{M,N}$. The following identity has been established:

$$W(g)e_v = \mu(\det g|_N)e_{gv}. \tag{5.8}$$

The linear character μ is completely determined in Lemma 3.1.3 and Theorem 3.1.4.

5.3 Computing P on Sp^N

In what follows u will denote an arbitrary element of M and v, w arbitrary elements of N. Set $S = S_\lambda$ and let $r \in R$. Then

$$S(0,w)e_v = (0,w)(0,v) \otimes y = (0, w+v) \otimes y = e_{v+w},$$

$$S(0,u)e_v = (0,u)(0,v) \otimes y = (0,v)(0,u) \otimes (2\langle u,v\rangle, 0)y = \lambda(2\langle u,v\rangle)e_v$$

and

$$S(r,0)e_v = (r,0)(0,v) \otimes y = (0,v) \otimes (r,0)y = \lambda(r)e_v.$$

The following formulae have been established

$$S(0,w)e_v = e_{v+w}, \tag{5.9}$$

$$S(0,u)e_v = \lambda(2\langle u,v\rangle)e_v, \tag{5.10}$$

$$S(r,0)e_v = \lambda(r)e_v. \tag{5.11}$$

Let $g \in \mathrm{Sp}^N$. Then $gx - x \in N$ for all $x \in V$ (Lemma 2.3.2(a)). Thus,

$$S^g(0,u) = S(0,gu) = S(0,gu-u+u) = S\left((0,gu-u)(0,u)(\langle u,gu\rangle,0)\right) \tag{5.12}$$

and

$$S^g(0,w) = S(0,gw) = S(0,w). \tag{5.13}$$

It follows from (5.9), (5.10), (5.12) and (5.13) that

$$S^g(0,u)e_v = \lambda(2\langle u,v\rangle + \langle u,gu\rangle)e_{v+(gu-u)}, \tag{5.14}$$

$$S^g(0,w)e_v = e_{v+w}. \tag{5.15}$$

Suppose that $P(g)$ has been found. Then $P(g)$ commutes with all the shift operators $S(0,w)$, and it is therefore determined by its action on e_0. More precisely,

$$P(g)e_v = S(0,v)P(g)e_0. \tag{5.16}$$

Since $P(g)$ is invertible,

$$x_0 = P(g)e_0 \neq 0. \tag{5.17}$$

Moreover,

$$S^g(0,u)x_0 = S^g(0,u)P(g)e_0 = P(g)S(0,u)e_0 = P(g)e_0 = x_0.$$

Thus

$$x_0 \text{ is a fixed point of all the operators } S^g(0,u),\ u \in M. \tag{5.18}$$

Conversely, suppose that $P(g) \in \mathrm{End}_F(X)$ satisfies (5.16), (5.17) and (5.18). Then

$$P(g) \neq 0 \tag{5.19}$$

due to (5.17) and

$$P(g)S(0,w) = S^g(0,w)P(g) \tag{5.20}$$

due to (5.9), (5.15) and (5.16). Moreover,

$$P(g)S(0,u) = S^g(0,u)P(g). \tag{5.21}$$

Indeed, from

$$(0,gu)(0,v) = (0,v)(0,-v)(0,gu)(0,v) = (2\langle gu,v\rangle,0)(0,v)(0,gu)$$

and

$$\langle gu,v\rangle = \langle (gu-u)+u,v\rangle = \langle u,v\rangle$$

we deduce

$$(0,gu)(0,v) = (2\langle u,v\rangle,0)(0,v)(0,gu),$$

whence

$$S^g(0,u)S(0,v) = \lambda(2\langle u,v\rangle)S(0,v)S^g(0,u) \tag{5.22}$$

upon applying S. Thus, in view of (5.10), (5.16), (5.18) and (5.22)

$$\begin{aligned} P(g)S(0,u)e_v &= \lambda(2\langle u,v\rangle)P(g)e_v = \lambda(2\langle u,v\rangle)S(0,v)x_0 \\ &= \lambda(2\langle u,v\rangle)S(0,v)S^g(0,u)x_0 = S^g(0,u)S(0,v)x_0 = S^g(0,u)P(g)e_v, \end{aligned}$$

as claimed. Given (5.19), (5.20), (5.21) and the fact that S is irreducible, Schur's Lemma yields that $P(g)$ is an invertible operator intertwining S and S^g.

Since S is absolutely irreducible, $P(g)$ is determined up to multiplication by a scalar. But $P(g)$ depends solely on x_0; thus, the fixed points of the group $S^g(0,u)_{u\in M}$ must be one-dimensional. This also follows from the facts that the fixed points of $S(0,u)_{u\in M}$ are equal to Fe_0 and that S is similar to S^g. We proceed to determine x_0.

Given $w \in \mathrm{Im}(g-1)$ there exists an element $u \in M$ satisfying

$$gu - u = w. \tag{5.23}$$

If $u' \in M$ also satisfies (5.23) then Lemma 2.3.2(b) gives

$$\langle u, w\rangle = \langle u, gu' - u'\rangle = \langle u', gu - u\rangle = \langle u', w\rangle.$$

Thus the expression $\langle u, w\rangle$ is independent of the choice of u. We shall denote by $u^{g,w} \in M$ an arbitrary element satisfying (5.23). We claim that

$$x_0 = \sum_{w \in \mathrm{Im}(g-1)} \lambda(\langle u^{g,w}, w\rangle) e_w \tag{5.24}$$

satisfies (5.18). Indeed, in view of (5.14)

$$S^g(0,u)x_0 = \sum_{w \in \mathrm{Im}(g-1)} \lambda(2\langle u, w\rangle + \langle u, gu\rangle + \langle u^{g,w}, w\rangle) e_{w+gu-u}. \tag{5.25}$$

Make the change of variables $w' = w + gu - u$; then the expression

$$2\langle u, w\rangle + \langle u, gu\rangle + \langle u^{g,w}, w\rangle,$$

appearing in (5.25), is transformed into

$$2\langle u, w'\rangle - 2\langle u, gu\rangle + \langle u, gu\rangle + \langle u^{g,w'-(gu-u)}, w' - (gu-u)\rangle. \tag{5.26}$$

Taking $u^{g,w'-(gu-u)} = u^{g,w'} - u$ the expansion of (5.26) becomes

$$2\langle u, w'\rangle - 2\langle u, gu\rangle + \langle u, gu\rangle + \langle u^{g,w'}, w'\rangle - \langle u^{g,w'}, gu - u\rangle - \langle u, w'\rangle + \langle u, gu\rangle,$$

which is nothing but $\langle u^{g,w'}, w'\rangle$, since

$$\langle u^{g,w'}, gu - u\rangle = \langle u, gu^{g,w'} - u^{g,w'}\rangle = \langle u, w'\rangle$$

due to Lemma 2.3.2(b). Thus (5.25) is equal to $\sum_{w' \in \mathrm{Im}(g-1)} \lambda(\langle u^{g,w'}, w'\rangle) e_{w'}$, as claimed. We have proven that, up to scaling,

$$P(g)e_v = \sum_{w \in \mathrm{Im}(g-1)} \lambda(\langle u^{g,w}, w\rangle) e_{v+w}. \tag{5.27}$$

5.3.1 Note To see how to arrive at (5.24), write an element x of X in terms of the basis $(e_v)_{v \in N}$ and force it to satisfy (5.18). Making use of Theorem 4.1.10 it can be shown that $x = x_0$, up to scaling. This is the reasoning that allowed the author to conjecture Theorem 4.1.10 in the first place.

5.4 Computing c on Sp^N

Let $g \in Sp^N$. Denote by $\hat{N}$ be the group of all linear characters $N^+ \to F^*$, and for each $\nu \in \hat{N}$ set $y_\nu = \sum_{w \in N} \nu(w) e_w$. A standard argument shows that $(y_\nu)_{\nu \in \hat{N}}$ is an F-basis of X that diagonalizes all the $S(0,w)$. In fact $(y_\nu)_{\nu \in \hat{N}}$ diagonalizes any commuting family of operators that contains all the $S(0,w)$; in particular $(y_\nu)_{\nu \in \hat{N}}$ diagonalizes $P(g)$.

Given $\nu \in \hat{N}$ denote by $-\nu$ the character $(-\nu)(w) = \nu(-w) = \nu(w)^{-1}$ and by 0 the trivial character $w \mapsto 1$. Let $(l^g_\nu)_{\nu \in \hat{N}}$ be the eigenvalues of $P(g)$ corresponding to the eigenvectors $(y_\nu)_{\nu \in \hat{N}}$. The very definitions of y_ν and $P(\iota)$ give

$$P(\iota) y_\nu = y_{-\nu}. \tag{5.28}$$

and, on the other hand, Proposition 3.3.2 guarantees that

$$P(\iota) P(g) = P(g) P(\iota). \tag{5.29}$$

The unconvinced reader might want to verify (5.29) directly. We deduce that

$$l^g_{-\nu} = l^g_\nu. \tag{5.30}$$

Indeed,

$$P(g) y_{-\nu} = P(g) P(\iota) y_\nu = P(\iota) P(g) y_\nu = l^g_\nu P(\iota) y_\nu = l^g_\nu y_{-\nu}.$$

Denote by $\hat{\mathcal{U}}$ a moiety of $\hat{N} \setminus \{0\}$. Then (5.28) shows that $(y_0, (y_\nu + y_{-\nu})_{\nu \in \hat{\mathcal{U}}})$ and $(y_\nu + y_{-\nu})_{\nu \in \hat{\mathcal{U}}}$ are basis of X_+ and X_-, respectively. Therefore (5.2) and (5.30) give

$$c(g) = (l^g_0)^{-1}; \tag{5.31}$$

here l^g_0 is the scalar satisfying $P(g) y_0 = l^g_0 y_0$, where $y_0 = \sum_{w \in N} e_w$. Using the definition (5.27) of $P(g)$ we discover that $P(g) y_0 = l^g_0 y_0$ forces

$$l^g_0 = \sum_{w \in \mathrm{Im}(g-1)} \lambda(\langle u^{g,w}, w \rangle). \tag{5.32}$$

Since $P(g)$ is invertible, its eigenvalue l^g_0 satisfies

$$l^g_0 \neq 0. \tag{5.33}$$

We have proven that

$$c(g) = \left(\sum_{w \in \mathrm{Im}(g-1)} \lambda(\langle u^{g,w}, w \rangle) \right)^{-1} \tag{5.34}$$

for all $g \in \mathrm{Sp}^N$.

5.5 Putting the pieces together

We specialize the above analysis to the elements $g^N(b)$, $b \in R^*$. By definition,

$$g^N(b)x = x + b\langle x, v_1 \rangle v_1 + \ldots + b\langle x, v_n \rangle v_n.$$

Thus

$$M \ni u \xrightarrow{g^N(b)-1} \sum_{1 \le i \le n} b\langle u, v_i \rangle v_i \in N$$

is a linear isomorphism. Given $w \in N$ the unique $u \in M$ satisfying (5.23) is given by

$$u = \sum_{1 \le i \le n} b^{-1} \langle u_i, w \rangle u_i.$$

Thus

$$\langle u, w \rangle = \sum_{1 \le i \le n} b^{-1} \langle u_i, w \rangle^2,$$

whence

$$P(g^N(b))e_v = \sum_{w \in N} \lambda \left(b^{-1} \sum_{1 \le i \le n} \langle u_i, w \rangle^2 \right) e_{v+w}.$$

Making the change of variables $w' = v + w$, (5.27) is finally transformed into

$$P(g^N(b))e_v = \sum_{w \in N} \lambda \left(b^{-1} \sum_{1 \le i \le n} \langle u_i, w - v \rangle^2 \right) e_w. \tag{5.35}$$

Moreover, (5.32) becomes

$$\begin{aligned} l_0^{g_1} &= \sum_{w\in N} \lambda\left(b^{-1}\sum_{1\le i\le n}\langle u_i, w\rangle^2\right) \\ &= \sum_{s_1,\dots,s_n\in R} \lambda\left(b^{-1}\sum_{1\le i\le n}\langle u_i, s_1v_1+\dots+s_nv_n\rangle^2\right) \\ &= \sum_{s_1,\dots,s_n\in R} \lambda\left(b^{-1}\sum_{1\le i\le n} s_i^2\right) \\ &= \sum (\lambda[b^{-1}])^n . \end{aligned} \tag{5.36}$$

In view of (5.33)

$$\sum(\lambda) \neq 0. \tag{5.37}$$

Thus (5.34), (5.35) and (5.36) give

$$W(g^N(b))e_v = \sum(\lambda[b^{-1}])^{-n}\sum_{w\in N}\lambda(b^{-1}\sum_{1\le i\le n}\langle u_i, w-v\rangle^2)e_w. \tag{5.38}$$

Recall that $g^M(-1)(x) = x + \langle x, u_1\rangle u_1 + \dots + \langle x, u_n\rangle u_n$. Then (5.4) gives

$$W(g^M(-1))e_v = \lambda(-\sum_{1\le i\le n}\langle v, u_i\rangle^2)e_v. \tag{5.39}$$

As a result of (2.12), (5.38) and (5.39) we finally obtain

$$W(g_{M,N})e_v = \sum(\lambda)^{-n}\sum_{w\in N}\lambda\left(-2\sum_{1\le i\le n}\langle u_i, w\rangle\langle u_i, v\rangle\right)e_w. \tag{5.40}$$

5.6 The final product

We are ready to state

5.6.1 Theorem The Weil representation $W = W_\lambda$ is defined as follows on the generators $\mathrm{Sp}_M, g_{M,N}, g^M(b)$ of Sp and the basis $(e_v)_{v\in N}$ of $X = X_M$:

$$W(g)e_v = \begin{cases} \mu(\det g|_N)e_{gv} & \text{if } g \in \mathrm{Sp}_{M,N} \\ \lambda(\langle gv, v\rangle)e_v & \text{if } g \in \mathrm{Sp}^M \\ \sum(\lambda)^{-n}\sum_{w\in N}\lambda\left(-2\sum_{1\le i\le n}\langle u_i, w\rangle\langle u_i, v\rangle\right)e_w & \text{if } g = g_{M,N} \\ \sum(\lambda[b^{-1}])^{-n}\sum_{w\in N}\lambda(b^{-1}\sum_{1\le i\le n}\langle u_i, w-v\rangle^2)e_w & \text{if } g = g^M(b). \end{cases} \tag{5.41}$$

5.6.2 Definition By *the* Weil Representation of Sp associated to λ we shall understand any representation of Sp similar to the one constructed in Theorem 5.6.1.

5.7 An alternative approach to compute quadratic sums

This section shows how one can use W itself to determine the quadratic sum $\sum(\lambda)$.

5.7.1 Proposition

$$\sum(\lambda) = \pm\sqrt{\mu(-1)|R|} \tag{5.42}$$

Proof: Set $n = 1$ in (5.41), so that N is one-dimensional over R. We obtain

$$W(g_{M,N})e_i = \sum(\lambda)^{-1}\sum_{j\in R}\lambda(-2ij)e_j$$

for all $i \in R$, whence

$$W(g_{M,N})^2 e_i = \sum(\lambda)^{-2}\sum_{t\in R}\sum_{j\in R}\lambda(-2j(i+t))e_t. \tag{5.43}$$

The linear character $j \mapsto \lambda(-2j(i+t))$ of R^+ is trivial if and only if $i + t = 0$, due to the primitivity of λ. Thus (5.43) and (5.8) give

$$(-1)^{1/2(|R|-1)}e_{-i} = W(\iota)e_i = W(g_{M,N}^2)e_i = \sum(\lambda)^{-2}|R|e_{-i}.$$

We have determined the quadratic sum $\sum(\lambda)$ up to a $\pm$ sign:

$$\sum(\lambda) = \pm\sqrt{(-1)^{1/2(|R|-1)}|R|} = \pm\sqrt{\mu(-1)|R|}.$$

□

It seems unlikely that the Weil representation can provide us with such detailed information about the sign in (5.42) as obtained in Section 3.2.

In order to establish (3.21) we shall recur to the group of symplectic similitudes GSp. An independent in-depth analysis of the interaction between GSp and W_λ is given in Section 7.3.

5.7.2 Proposition GSp transitively permutes the Weil characters of Sp. In fact,

$$W_\lambda^{B_k} = W_{\lambda[k]}. \tag{5.44}$$

for all units $k \in R$.

Proof: In view of (2.16) the action of GSp on the Weil characters is determined by the B_k's. In light of Lemma 3.2.4 the Weil characters are the characters of $(W_{\lambda[k]})_{k\in R^\bullet}$.

We shall verify (5.44) on the generators Sp_M, $(g^N(b))_{b\in R^\bullet}$ of Sp, given in Corollary 2.3.8. Let $v \in N$.

Case 1. $g \in \mathrm{Sp}_{M,N}$. Then ${}^{B_k}gv = gv$, hence (2.19) and (2.20) give

$$W_\lambda^{B_k}(g)e_v = \mu(\det g|_N)e_{gv} = W_{\lambda[k]}(g)e_v.$$

Case 2. $g \in \mathrm{Sp}^M$. Then

$${}^{B_k}gv = B_k gv = B_k((gv - v) + v) = k(gv - v) + v,$$

so that

$$\langle {}^{B_k}gv, v\rangle = k\langle gv, v\rangle,$$

whence

$$W_\lambda^{B_k}(g)e_v = \lambda(k\langle gv, v\rangle)e_v = W_{\lambda[k]}(g)e_v.$$

Case 3. If $g = g^N(b)$. Then (2.21) gives

$$W_\lambda^{B_k}(g)e_v = W_\lambda(g^N(k^{-1}b))e_v = \sum \left(\lambda[kb^{-1}]\right)^{-n} \sum_{w\in N} \lambda(kb^{-1} \sum_{1\le i\le n} \langle u_i, w - v\rangle^2)e_w$$

$$= W_{\lambda[k]}(g)e_v.$$

The relation (5.44) has been established. □

As a corollary of Theorem 5.6.1 and Proposition 5.7.2 we finally obtain

5.7.3 Proposition

$$\sum(\lambda[k]) = \mu(k)\sum(\lambda) \tag{5.45}$$

for all units $k \in R$.

In view of (2.18) and Proposition 5.7.2, we have

$$W_{\lambda[k]}(g_{M,N}) = W_\lambda({}^{B_k}g_{M,N}) = W_\lambda(g_k g_{M,N}) = W_\lambda(g_k)W_\lambda(g_{M,N}). \tag{5.46}$$

Set $n = 1$ in (5.41), so that N is one-dimensional over R. Then (5.46) reads:

$$\sum(\lambda[k])^{-1}\sum_{j\in R}\lambda(-2kij)e_j = \mu(k^{-1})\sum(\lambda)^{-1}\sum_{j\in R}\lambda(-2ij)e_{k^{-1}j} \tag{5.47}$$

for all $i \in R$. But the right hand side of (5.47) is equal to

$$\Big(\mu(k)\sum(\lambda)\Big)^{-1}\sum_{j\in R}\lambda(-2kij)e_j,$$

whence

$$\sum(\lambda[k]) = \mu(k)\sum(\lambda).$$

□

5.8 Uniqueness of the Weil Representation revisited

Assume here that R is an irreducible ring. We come back to the uniqueness question to see how one can tell *the* Weil Representation apart when Sp *is* imperfect.

5.8.1 Lemma If Sp is imperfect there are precisely three types of Weil representations of associated to λ, in the sense of Definition 4.7. The Weil representation, in the sense of Definition 5.6.2, is the only one of the three whose character Ω satisfies:

$$\Omega(\rho_{1,u_1}) = |R|^{n-1}\sum(\lambda) \tag{5.48}$$

Proof: It was shown in (5.6) that Ω satisfies (5.48).

Suppose that $\hat{W}$ also satisfies (4.7). Again, given the absolute irreducibility of S, $W = \tau\hat{W}$, for some linear character τ of Sp. In view of Corollary 2.4.4 we have $\tau = \tau_i$ for some $i, 0 \leq i < 3$. Denote by $\hat{\Omega}$ the character of $\hat{W}$. If we force $\hat{\Omega}$ to also satisfy (5.48) then

$$\sum(\lambda) = \Omega(\rho_{1,u_1}) = \tau\hat{\Omega}(\rho_{1,u_1}) = \zeta_3^i \sum(\lambda)\,. \tag{5.49}$$

But (5.37) gives $\sum(\lambda) \neq 0$. Thus, (5.49) forces $i = 0$, whence $\tau = 1$. □

Chapter 6

FSp-submodules of X

Assume here that R is an irreducible ring. In preparation for the study of the irreducible FSp-components of X, we present here several useful tools in defining, constructing and handling FSp-submodules of X.

6.1 The FSp-submodules $X(I)$ of X

Of course, X itself cannot be irreducible since the ± 1-eigenspaces of $W(\iota)$ are FSp-submodules.

We state the following immediate consequence of Lemma 4.2.5 and Theorem 4.2.6 in order to be absolutely precise about the action of $W(\iota)$ on X.

6.1.1 Corollary Let $L \in \mathcal{L}$, $X = X_L$ and $\mathcal{T} = \mathcal{T}(V/L)$. Then the action $W(\iota)$ of ι on X is given by

$$W(\iota)e_v = \mu(-1)^n e_{-v}, \quad v \in \mathcal{T} \tag{6.1}$$

and the character value of ι is equal to

$$\Omega(\iota) = \mu(-1)^n. \tag{6.2}$$

Definition 5.6.2 is not required here because any linear character of Sp is trivial on ι (Corollary 2.4.4). We shall henceforth denote by $X^{\pm}$ the ± 1-eigenspaces of X relative to

$W(\iota)$. In the case $R = F_q$, they exhaust all the proper submodules of X. In general, this is far from true, as explained below.

As a general principle, if S is any subset of $H \rtimes \mathrm{Sp}$ normalized by Sp then the fixed points X^S of S in X form an FSp-submodule. In the sequel we shall be only interested in the following cases.

- $S = \mathrm{Sp}(I) = \{g \in \mathrm{Sp} \mid gv \equiv v \mod IV\}$, the congruence subgroup of Sp associated to the ideal I of R.
- $S = D(I) = (0, IV)$, the abelian subgroup of H corresponding to a given ideal I of R of square (0).
- $S = E(I) = (R, IV)$, the subgroup of H corresponding to a given ideal I of R.

We shall fix an A-pair (I, J) until the end of this section. By far the most important A-pair when R is not a field is $(\mathfrak{min}, \mathfrak{m})$. Denote by $X(I) = X^{D(I)}$ the fixed points of $D(I)$ in X and by $Y(I)$ the FSp-module $X/X(I)$, or any FSp-submodule of X complementing $X(I)$. Since $N_H(D(I)) = C_H(D(I)) = E(J)$, $X(I)$ is an $F(E(J)/X(I))$-module. Given a FSp-submodule Z of X let $W_{\lambda,Z}$ and $\Omega_{\lambda,Z}$ be corresponding Weil objects attached to Z, and let $Z^{\pm}$ be the FSp-submodules $Z \cap X^{\pm}$. The most important modules for us are $X(\mathfrak{min})$ and $Top^{\pm}$, where $Top = Y(\mathfrak{min})$ if R is not a field and $Top = X$ otherwise.

The following result is extremely useful in dealing with $X(I)$. It was originally proved in collaboration with Gerald Cliff and David A. McNeilly for a principal ring R.

6.1.2 Proposition Let G be any subgroup of H satisfying $(J^2, JV) \subseteq G \subseteq E(J)$. Then $X = \mathrm{ind}_{E(J)}^H X(I)$, whence $X(I)$ is an absolutely irreducible $F(G/D(I))$-module of dimension $|J/I|^n$.

Proof: Take any $A = (R, L) \in \mathcal{A}$ containing $E(I)$. In view of Corollary 4.1.8 ρ_0 enters $\eta|_A$, whence $E(I) \ni (r, v) \xrightarrow{\tau} \lambda(r) \in F^*$ enters $\eta|_{E(I)}$. Corollary 4.1.3 and Lemma 2.3.1 show that the inertia group of τ is precisely $E(J)$. Thus, by Clifford theory, $X = \mathrm{ind}_{E(J)}^H Z$, where $Z = \{x \in X \mid (r, v)x = \lambda(r) \text{ for all } (r, v) \in E(I)\}$ is an absolutely irreducible $FE(J)$-module. Note however that $Z = X(I)$ and that $(R, 0)$ acts by scalar multiplication on X. Thus $X = \mathrm{ind}_{E(J)}^H X(I)$ and $X(I)$ is an absolutely irreducible $F(G/D(I))$-module,

for any G as above. (Eq. 3.15) finally gives

$$\dim X(I) = \dim X \frac{|E(J)|}{|H|} = |R|^n \frac{|R||J|^{2n}}{|R|^{2n+1}} = |J/I|^n.$$

□

6.1.3 Lemma $\Omega_{X(I)}(\iota) = \mu(-1)^n$. Thus $\dim Y(I)^+ = \dim Y(I)^- = (|R|^n - |J/I|^n)/2$ and $\dim X(I)^\pm = (|J/I|^n \pm \mu(-1)^n)/2$.

Proof: Let $L = L_{I,J} = IN \oplus JM$, $X = X_L$ and $P = P_L$. Construct $\mathcal{T} = \mathcal{T}(V/L)$ so that it contains a transversal $\mathcal{T}_{I,J}$ of JN relative to IN. For each $v \in \mathcal{T}_{I,J}$ and $(0,w) \in D(I)$ we have

$$(0,w)e_v = (0,w)(0,v) \otimes y = (0,v)(0,w) \otimes y = (0,v) \otimes (0,w)y = (0,v) \otimes y = e_v.$$

Since $\dim X(I) = |J/I|^n = |\mathcal{T}_{I,J}|$, $(e_v)_{v \in \mathcal{T}_{I,J}}$ is indeed a basis of $X(I)$. Thus (6.1) gives

$$\Omega_{X(I)}(\iota) = \mu(-1)^n. \tag{6.3}$$

As a consequence of (6.2) and (6.3) we obtain

$$\Omega_{Y(I)}(\iota) = 0. \tag{6.4}$$

Since $W(\iota)^2 = 1$, (6.3) and (6.4) give

$$\dim X(I)^\pm = (|J/I|^n \pm \mu(-1)^n)/2$$

and

$$\dim Y(I)^+ = \dim Y(I)^- = (|R|^n - |J/I|^n)/2.$$

□

6.1.4 Lemma Suppose that $I = J$. Then Sp acts trivially on the one-dimensional FSp-module $X(I)$. Moreover, if $L = IV$ then $\mathrm{Sp}_L = \mathrm{Sp}$ and $P_L = W_\lambda$.

Proof: Since Sp preserves L, $\mathrm{Sp} = \mathrm{Sp}_L$. The dimension of $X(I)$ is given in Proposition 6.1.2. By definition, P gives a Weil representation associated to λ. Thus, P must be equal to W_λ if Sp is perfect, in which case Sp acts trivially on $X(I)$, since $\dim X(I) = 1$.

At any rate, if $X = X_L$ and $P = P_L$ then P satisfies

$$P(g)e_0 = \lambda(\langle g0, 0\rangle)e_0 = e_0$$

for all $g \in \mathrm{Sp}$, whence Sp acts trivially on $X(I)$ via P. It remains to verify that P satisfies (5.48). To see this, let $g = \rho_{1,u_1}$ and $\mathcal{T}_I = \mathcal{T}(R/I)$, $\mathcal{T} = \mathcal{T}(V/IV) = (tu_1 + sv_1)_{s,t\in\mathcal{T}_I}$. Then $gv \equiv v \mod IV$ for some $v \in \mathcal{T}$ if and only if $v = tu_1$ for some $t \in \mathcal{T}_I$. Thus (4.10), (3.15) and (3.19) give

$$\mathrm{tr}(P(g)) = \sum_{t\in\mathcal{T}_I} \lambda(\langle tu_1, tu_1\rangle) = |\mathcal{T}_I| = |R/I| = \sqrt{|R|} = \sum(\lambda),$$

as desired. □

6.2 $X(I)$ via idempotents of $F(H \rtimes \mathrm{Sp})$

Making a slight change in the point of view, we approach the study of the FSp-modules $X(I)$ and $Y(I)$ via Sp-invariant idempotents of $F(H \rtimes \mathrm{Sp})$.

We begin by introducing some notation. Denote by $h(I)$ the idempotent of $FH \subseteq F(H \rtimes \mathrm{Sp})$ associated to $D(I)$; that is

$$h(I) = \frac{1}{|D(I)|}\sum_{h\in D(I)} h = \frac{1}{|I|^{2n}}\sum_{w\in IV}(0,w) = \frac{1}{|I|^{2n}}\sum_{w\in IN}(0,w)\sum_{u\in IM}(0,u). \tag{6.5}$$

Since $D(I)$ is normalized by Sp, $h(I)$ is Sp-invariant. Similarly, let $(1+\iota)/2$ be the idempotent of $\mathrm{FSp} \subseteq F(H \rtimes \mathrm{Sp})$ associated to the central subgroup $\{1, \iota\}$ of Sp. Denote by SW the Weil representation $H \rtimes \mathrm{Sp} \to \mathrm{GL}(X)$ defined by $SW(hg) = S(h)W(g)$ and use the same symbol to denote its linear extension to the corresponding F-algebra homomorphism $F(H \rtimes \mathrm{Sp}) \to \mathrm{End}_F(X)$. By abuse of notation, we shall write $h(I) = SW(h(I))$, $(1+\iota)/2 = SW((1+\iota)/2)$ and $(1-\iota)/2 = SW((1-\iota)/2)$. Accordingly, $1 - h(I)$, $h(I)$, $\frac{1+\iota}{2}$ and $\frac{1-\iota}{2}$ are commuting projections in $\mathrm{End}_{\mathrm{FSp}}(X)$ satisfying:

$$X(I) = h(I)X, \quad Y(I) = (1-h(I))X, \quad Z^+ = \frac{1+\iota}{2}Z \quad \text{and} \quad Z^- = \frac{1-\iota}{2}Z \tag{6.6}$$

for all FSp-submodules Z of X. We shall distinguish elements of $F(H \rtimes \mathrm{Sp})$ from elements of $\mathrm{End}_F(X)$ by the context.

We proceed to produce bases of $X(I)^{\pm}$ and $Y(I)^{\pm}$, that will prove useful in the sequel. We treat first the model $X = X_M$. One of the aims is to show that the matrices of $W_{X(I)^{\pm}}(g)$ and $W_{Y(I)^{\pm}}(g)$ relative to these bases have rational entries, for all $g \in \mathrm{Sp}_{M,N}$. This will constitute the first step in the process of realizing $W_{Top^{\pm}}(g)$ over a minimal field.

Set $X = X_M$. Given $v \in N$ we have

$$h(I)e_v = \frac{1}{|I|^{2n}} \sum_{w \in IN} (0,w) \left(\sum_{u \in IM} \lambda(2\langle u,v \rangle) \right) e_v, \tag{6.7}$$

due to (6.5) and (5.10). In view of Corollary 4.1.2 the linear character $u \mapsto \lambda(2\langle u,v \rangle)$ of IM is trivial if and only if $v \in JN$, whence (6.7) and (5.9) give

$$\widehat{e_v} = h(I)e_v = \begin{cases} \frac{1}{|I|^n} \sum_{w \in IN} e_{v+w} & \text{if } v \in JN, \\ 0 & \text{otherwise,} \end{cases} \tag{6.8}$$

an equation originally obtained by David A. McNeilly. In virtue of (6.6), the vectors

$$(\frac{1 \pm \iota}{2} h(I)e_v)_{v \in N} \tag{6.9}$$

generate $X(I)^{\pm}$, while

$$(\frac{1 \pm \iota}{2}(1 - h(I))e_v)_{v \in N} \tag{6.10}$$

generate $Y(I)^{\pm}$. Thus, in view of Proposition 6.1.2

$$\mathcal{B}(I) = (\widehat{e_v})_{v \in \mathcal{T}(JN/IN)} \tag{6.11}$$

must be a basis of $X(I)$. Let $\mathcal{S}(JN/IN)$ be a moiety of $\mathcal{T}(JN/IN) \setminus \{0\}$. Then

$$\mathcal{B}(I)^{+} = \frac{1+\iota}{2}(\widehat{e_v})_{v \in \mathcal{S}(JN/IN)} \cup \begin{cases} \{e_0\} & \text{if } \mu(-1)^n = 1 \\ \emptyset & \text{otherwise} \end{cases} \tag{6.12}$$

is a basis of $X(I)^{+}$ and

$$\mathcal{B}(I)^{-} = \frac{1-\iota}{2}(\widehat{e_v})_{v \in \mathcal{S}(JN/IN)} \cup \begin{cases} \{e_0\} & \text{if } \mu(-1)^n = -1 \\ \emptyset & \text{otherwise} \end{cases} \tag{6.13}$$

is a basis of $X(I)^-$.

Extract bases $\mathcal{C}(I)^\pm$ of $Y(I)^\pm$ by removing redundant vectors from (6.10), starting in any order. Then the matrix of change of basis from $(e_v)_{v\in N}$ to $\mathcal{B}(I)^+\cup\mathcal{B}(I)^-\cup\mathcal{C}(I)^+\cup\mathcal{C}(I)^-$ has rational entries, since all vectors appearing in (6.9) and (6.10) are rational linear combinations of the basis vectors $(e_v)_{v\in N}$, due to (6.8).

On the other hand, the matrix of any $W(g)$, $g\in \mathrm{Sp}_{M,N}$, has rational entries relative to the basis $(e_v)_{v\in N}$, due to (5.8). We have thus proven

6.2.1 Lemma The matrices of $W_{X(I)^\pm}(g)$ and $W_{Y(I)^\pm}(g)$ relative the bases $\mathcal{B}(I)^\pm$ and $\mathcal{C}(I)^\pm$ have rational entries, for all $g\in \mathrm{Sp}_{M,N}$.

Substitute $I=(0)$ in Lemma 6.2.1 when R is a field and $I=\min$ otherwise. We obtain

6.2.2 Corollary The matrices of $W_{Top^\pm}(g)$ relative to the bases

$$\begin{cases} \mathcal{B}(0)^\pm & \text{if } R \text{ is a field} \\ \mathcal{C}(\min)^\pm & \text{otherwise} \end{cases} \tag{6.14}$$

have rational entries for all $g\in \mathrm{Sp}_{M,N}$.

In the next result, we locate $X(\min)$ and $Top^\pm$ within other models of X.

6.2.3 Proposition Suppose that (I,J) is a non-trivial A-pair. Set $L=L_{I,J}$ and $X=X_L$. Given $\mathcal{T}=\mathcal{T}(V/L)$, let $\mathcal{T}_{L,\mathfrak{m}}$ be the transversal of $\mathfrak{m}V$ relative to L contained within it. Set $\mathcal{P}_0=\mathcal{T}\setminus\mathcal{T}_{L,\mathfrak{m}}$ and let $\mathcal{S}_0$ be a moiety of $\mathcal{P}_0$. Then

(a) $(e_v)_{v\in\mathcal{S}}$ is a basis of $X(\min)$.

(b) $(e_v)_{v\in\mathcal{P}_0}$ is a basis of Top and $(\frac{1\pm\iota}{2}e_v)_{v\in\mathcal{S}_0}$ are bases of $Top^\pm$.

Proof:

(a) We have $|\mathcal{T}_{L,\mathfrak{m}}|=|\mathfrak{m}/I|^n|\mathfrak{m}/J|^n$. On the other hand, $|I||J|=|R|=|\min||\mathfrak{m}|$, due to (3.15). Thus $|\mathcal{T}_{L,\mathfrak{m}}|=|\mathfrak{m}/\min|^n$, which is equal to $\dim X(\min)$, in view of Proposition 6.1.2. It thus suffices to show that every e_v, $v\in\mathcal{T}_{L,\mathfrak{m}}$ is fixed by every $(0,w)\in D(\min)$. Well,

$$(0,w)e_v=(0,w)(0,v)\otimes y=(0,v)(0,w)\otimes y=(0,v)\otimes(0,w)y=(0,v)\otimes y=e_v,$$

since $\mathfrak{m} \cdot \min = (0)$ and $D(\min) \subseteq (0, L)$.

(b) There is a priori no reason why $(e_v)_{v \in \mathcal{P}_0}$ should generate an FSp-stable submodule. We shall prove that each e_v, $v \in \mathcal{P}_0$, is in the kernel of $h(\min)$, whence $\mathrm{span}(e_v)_{v \in \mathcal{P}_0} = \mathrm{Ker}\, h(\min)$. For $v \in \mathcal{P}_0$ and $(0, w) \in D(\min)$ we have

$$(0, w)e_v = (0, w)(0, v) \otimes y = (0, v)(0, w)(2\langle w, v\rangle, 0) \otimes y = \lambda(2\langle w, v)e_v,$$

since $D(\min) \subseteq (0, L)$. Fix $v \in \mathcal{P}_0$ and consider the linear character $w \mapsto \lambda(2\langle w, v\rangle)$ of $\min V$. Since v is primitive, this is not the trivial character, whence

$$h(\min)e_v = \left(\frac{1}{|D(\min)|} \sum_{w \in \min V} (0, w)\right) e_v = \left(\frac{1}{|D(\min)|} \sum_{w \in \min V} \lambda(2\langle w, v\rangle)\right) e_v = 0,$$

as required. The last assertion is consequence of Lemma 6.1.3. □

6.3 Explicit decompositions of X

We produce decompositions of $X^{\pm}$ (and hence X) into (non-isomorphic) FSp-submodules of strictly descending dimensions, starting from strictly ascending chains of A-pairs of R. When R is principal this gives *the* decomposition of X into $l + 1$ absolutely irreducible FSp-submodules.

The idea is to start from a decomposition of $1 \in F(H \rtimes \mathrm{Sp})$ into orthogonal Sp-invariant idempotents and produce a decomposition of $1 \in \mathrm{End}_{\mathrm{FSp}}(X)$ into orthogonal projections, via the Weil representation. Of course, one has to check what non-zero idempotents of $F(H \rtimes \mathrm{Sp})$ yield non-zero projections in $\mathrm{End}_{\mathrm{FSp}}(X)$.

Given A-pairs (I, J) and (I', J'), the idempotents $h(I)$ and $h(I')$ satisfy the usual relations:

$$(I, J) \leq (I', J') \Rightarrow h(I)h(I') = h(I') = h(I')h(I). \tag{6.15}$$

We shall write $h(I, I')$ for the Sp-invariant idempotent $h(I) - h(I') \in F(H \rtimes \mathrm{Sp})$ and, by abuse of notation, also by $h(I, I')$ the projection $h(I) - h(I') \in \mathrm{End}_{\mathrm{FSp}}(X)$.

Let $t \geq 0$ be an integer. Given a strictly ascending chain $\mathcal{C}$ of A-pairs

$$(0, R) = (I_0, J_0) < (I_1, J_1) < \ldots < (I_t, J_t) \tag{6.16}$$

write the decompositions $\mathcal{D}^{\pm}(\mathcal{C})$ of of $\frac{1\pm\iota}{2}$ (and hence 1) as follows:

$$\frac{1\pm\iota}{2} = \frac{1\pm\iota}{2}h(I_0, I_1) + \ldots + \frac{1\pm\iota}{2}h(I_{t-1}, I_t) + \frac{1\pm\iota}{2}h(I_t).$$

Apply SW and denote also by $\mathcal{D}^{\pm}(\mathcal{C})$ the resulting decompositions of $\frac{1\pm\iota}{2} \in \mathrm{End}_{\mathrm{FSp}}(X)$ into orthogonal projections belonging to $\mathrm{End}_{\mathrm{FSp}}(X)$.

6.3.1 Proposition The decompositions $\mathcal{D}^{\pm}(\mathcal{C})$ of $\frac{1\pm\iota}{2} \in \mathrm{End}_{\mathrm{FSp}}(X)$ satisfy:

(a) $\dim_F \frac{1\pm\iota}{2}h(I_i, I_{i+1})X = \dim_F \frac{1-\iota}{2}h(I_i, I_{i+1})X = (|J_i/I_i|^n - |J_{i+1}/I_{i+1}|^n)/2$ for all $0 \le i < t$.

(b) $\dim_F \frac{1\pm\iota}{2}h(I_t)X = (|J_t/I_t|^n \pm \mu(-1)^n)/2$.

(c) Any member of $\mathcal{D}^{+}(\mathcal{C})$ is orthogonal to any $\mathcal{D}^{-}(\mathcal{C})$.

(d) If $0 \le i < t-1$ then

$$\dim_F \frac{1+\iota}{2}h(I_i, I_{i+1}) > \dim_F \frac{1+\iota}{2}h(I_{i+1}, I_{i+2}),$$

while

$$\dim_F \frac{1+\iota}{2}h(I_i, I_{i+1}) > \dim_F \frac{1+\iota}{2}h(I_t)$$

for all $0 \le i < t$.

Proof: (a) and (b) follow from Proposition 6.1.2 and Lemma 6.1.3, while (c) is obvious. It remains to prove (d). Since $I_i \subsetneq I_{i+1} \subsetneq J_{i+1} \subsetneq J_i$ we have $|I_{i+1}| \ge q|I_i|$ and $|J_i| \ge q|J_{i+i}|$, whence Lemma 2.2.1(b) gives

$$|J_i/I_i|^n \ge q^{2n}|J_{i+1}/I_{i+1}|. \tag{6.17}$$

Combining (6.17) with (a) we obtain (d). □

Thus the $i-th$ projections in $\mathcal{D}^{+}(\mathcal{C})$ and $\mathcal{D}^{-}(\mathcal{C})$ have the same rank, except for the $t-th$ projections which differ by 1, while within each decomposition $\mathcal{D}^{\pm}(\mathcal{C})$ the projections strictly decrease in rank. Denote by $\mathbf{T}(\mathcal{C})$ the combined total of non-zero projections in $\mathcal{D}^{\pm}(\mathcal{C})$ arising from the chain $\mathcal{C}$. Then

$$\mathbf{T}(\mathcal{C}) = \begin{cases} 2(t+1)-1 & \text{if } I_t = J_t \\ 2(t+1) & \text{if } I_t \ne J_t. \end{cases} \tag{6.18}$$

6.4 Some character values

6.4.1 Lemma If Z is any FSp-submodule of X then $\Omega_{Z^\pm}(g) = (\Omega_Z(g) \pm \Omega_Z(\iota g))/2$ for all $g \in \mathrm{Sp}$.

Proof: Given $g \in \mathrm{Sp}$ we have

$$\Omega_Z(g) = \Omega_{Z^+}(g) + \Omega_{Z^-}(g)$$

$$\Omega_Z(\iota g) = \Omega_{Z^+}(g) - \Omega_{Z^-}(g),$$

whence $\Omega_{Z^\pm}(g) = (\Omega_Z(g) \pm \Omega_Z(\iota g))/2$. □

6.4.2 Lemma If $g \in \mathrm{Sp}^M$ then $\Omega(\iota g) = \mu(-1)^n$.

Proof: Let $X = X_M$ and $\mathcal{T} = \mathcal{T}(V/M) = N$. Then Theorem 5.6.1 gives

$$W(\iota g)e_v = \mu(-1)^n \lambda(\langle gv, v\rangle)e_{-v}$$

for all $v \in N$, whence $\Omega(\iota g) = \mu(-1)^n$. □

6.4.3 Lemma Let I be an ideal of R, $J = ((0) : I)$ and $K = (I : J)$. If $g \in \mathrm{Sp}(K)$ then $\Omega_{X(I)}(\iota g) = \mu(-1)^n$.

Proof: In view of Theorem 7.1.1 $W(g)|_{X(I)} = 1_{X(I)}$. Thus $\Omega_{X(I)}(\iota g) = \Omega_{X(I)}(\iota) = \mu(-1)^n$, due to Lemma 6.1.3. □

Chapter 7

Fundamental properties of the Weil Representations

Assume here that R is an irreducible ring.

7.1 The congruence subgroup $\mathrm{Sp}(K)$ acts trivially on $X(I)$

The next result is of great importance for us. It was originally proved in collaboration with Gerald Cliff and David A. McNeilly for a principal ring R.

7.1.1 Theorem Let (I, J) be an A-pair and denote by $K = (I : J)$ the conductor of J into I. Then the congruence subgroup $\mathrm{Sp}(K)$ acts trivially on $X(I)$.

1^{st} Proof (Independent of the appearance of W): Observe that $X(I)$ is an $E(J) \rtimes \mathrm{Sp}$ and hence $E(J)/D(I) \rtimes \mathrm{Sp}$-module. Also, the action of $\mathrm{Sp}(K)$ on $E(J)/D(I)$ is trivial, thereby yielding the action

$$\overline{g}\,\overline{h} = \overline{gh}$$

of Sp_K on $E(J)/D(I)$. But $X(I)$ is an absolutely irreducible $F(E(J)/D(I))$-module, whence $\mathrm{Sp}(K)$ acts by a linear character on $X(I)$. We thus obtain a representation

$$\mathrm{Sp}_K \ni \overline{g} \mapsto W(g)|_{X(I)}F^* \in \mathrm{PGL}(X(I)),$$

and hence a lift $\overline{P} : \mathrm{Sp}_K \to \mathrm{GL}(X(I))$, which is a projective representation satisfying

$$\overline{P}(\overline{g})\overline{S}(\overline{h})\overline{P}(\overline{g})^{-1} = \overline{S}(\overline{{}^g h}) = \overline{S}(\overline{{}^g h}). \tag{7.1}$$

Here $\overline{S}(\overline{h}) = S(h)|_{X(I)}$ for all $h \in E(J)$ and corresponding $\overline{h} \in E(J)/D(I)$.

We specifically choose $\overline{P}(\overline{\iota}) = P(\iota)|_{X(I)}$, where P is as defined in Lemma 6.1.3. Then the ± 1-eigenspaces of $\overline{P}(\overline{\iota})$ have dimensions $(|J/I|^n \pm 1)/2$ and $\mathrm{tr}(\overline{P}(\overline{\iota})) = 1$.

It follows from Propositions 3.3.1 and 3.3.2 applied to $z = \overline{\iota}$ that $\overline{P}$ can be corrected to an ordinary representation; that is, there is a representation $\overline{W} : \mathrm{Sp}_K \to \mathrm{GL}(X(I))$ satisfying (7.1). Inflate $\overline{W}$ to Sp by means of $W_0(g) = \overline{W}(\overline{g})$ obtaining the equation

$$W_0(g)S(h)|_{X(I)}W_0(g)^{-1} = S({}^g h)|_{X(I)}$$

for all $g \in \mathrm{Sp}$ and $h \in E(J)$. Since $X(I)$ is an absolutely irreducible $FE(J)$-module

$$W(g)|_{X(I)}\tau(g) = W_0(g), \qquad g \in \mathrm{Sp} \tag{7.2}$$

for some linear character τ of Sp. Apply (7.2) to any $g \in \mathrm{Sp}(K)$. Three cases arise:

Case 1. Sp is perfect. Then $W_0(g) = \tau(g) = 1$ and therefore $W(g)|_{X(I)} = 1$.

Case 2. Sp is imperfect but $I \neq J$. Then $K \subseteq \mathfrak{m}$ and a fortiori, $\mathrm{Sp}(K) \subseteq \mathrm{Sp}'$ (Proposition 2.4.3). Thus $W(g)|_{X(I)} = 1$, as above.

Case 3. Sp is imperfect and $I = J$. Then Lemma 6.1.4 gives that $\mathrm{Sp} = \mathrm{Sp}(K)$ acts trivially on $X(I)$.

2^{nd} Proof (Based on the appearance of W): In view of Corollary 2.2.7, $\mathrm{Sp}(K)$ acts trivially on $X(I)$ provided all $(\rho_{r,x})_{r\in K}$ act trivially on $X(I)$ for some $x \in \mathcal{P}$. To verify this, let $v \in N$ and $g \in \mathrm{Sp}^M \cap \mathrm{Sp}(K)$ (e.g. $g = \rho_{r,u_1}$, $r \in K$). Then

$$W(g)h(I)e_v = h(I)W(g)e_v = \lambda(\langle gv, v\rangle)h(I)e_v \tag{7.3}$$

due to (5.4). Since $\mathrm{Sp}(K)$ acts trivially on JV/IV, we have

$$\lambda(\langle gv, v\rangle) = 1$$

for all $v \in JV$, whence

$$W(g)h(I)e_v = h(I)e_v$$

for all $v \in N$, due to (7.3) and (6.8). □

7.2 The FSp-isomorphism $\widehat{JV/IV} \simeq \mathrm{End}_F(X(I))$

We have come to one of the most important results concerning Weil representations and this thesis.

Given a permutation representation $G \to Sym(\Delta)$ of a group G, we shall denote by $G \to \mathrm{GL}(\widehat{\Delta})$ the corresponding F-linear representation. Thus $\widehat{\Delta}$ has a basis $(f_x)_{x\in\Delta}$ and G acts on $\widehat{\Delta}$ by means of ${}^g f_x = f_{gx}$.

7.2.1 Theorem Let (I, J) be any A-pair. Then

$$\widehat{JV/IV} \ni f_{v+IV} \to S(0,v)|_{X(I)} \in \mathrm{End}_F(X(I)) \tag{7.4}$$

defines an isomorphism of FSp-modules.

Proof: The map (7.4) is well defined since $X(I)$ is preserved by $E(J)$ and acted upon trivially by $D(I)$. Given $g \in \mathrm{Sp}$ and $v \in JV$ we have

$$\begin{aligned} {}^g f_{v+IV} = f_{gv+IV} \mapsto S(0,gv)|_{X(I)} &= S({}^g(0,v))|_{X(I)} \\ &= W(g)|_{X(I)} S(0,v)|_{X(I)} W(g)|_{X(I)}^{-1} = {}^g S(0,v)|_{X(I)}. \end{aligned}$$

Since $X(I)$ is an absolutely irreducible $FE(J)$-module, the Jacobson density theorem ensures that the F-span of the $S(0,v)$ is all of $\mathrm{End}_F(X(I))$. Thus (7.4) is an epimorphism, and therefore a monomorphism, since the dimensions match (Proposition 6.1.2). □

7.2.2 Corollary Let (I, J) be any A-pair and denote by K the conductor of J into I. Then the kernel of the representation $\mathrm{Sp} \to GL(X(I))$ is precisely $\mathrm{Sp}(K)$. In particular, the Weil representation is faithful.

Proof: If $g \in \mathrm{Sp}$ acts trivially on $X(I)$ then g acts trivially on $\mathrm{End}_F(X(I))$ and hence on $\widehat{JV/IV}$. This readily implies that $g \in \mathrm{Sp}(K)$. The reverse inclusion is the content of Theorem 7.1.1. □

7.2.3 Corollary Let (I, J) be any A-pair. Then

$$[\Omega|_{X(I)}, \Omega|_{X(I)}] = o(JV/IV). \tag{7.5}$$

Proof: Passing to the fixed points in (7.4) we deduce that $\mathrm{End}_F(X(I))$ and $\widehat{JV/IV}$ contain the trivial representation an equal number of times, which is a restatement of (7.5). □

As a consequence of (7.5) we obtain the following fundamental result:

7.2.4 Theorem *$Top^{\pm}$ are absolutely irreducible FSp-modules of common degree*

$$\begin{cases} (|R|^n - |\mathrm{m/min}|^n)/2 & \text{if } R \text{ is not a field} \\ (q^n \pm (\frac{-1}{q})^n)/2 & \text{if } R = F_q. \end{cases}$$

and multiplicity one in X.

Proof: The degrees of $Top^{\pm}$ are given in Lemma 6.1.3. We divide the rest of the proof into two cases.

Case 1. R is a field. We have

$$\begin{aligned} 2 &= o(V), \quad \text{Lemma 2.6.1} \\ &= [\Omega, \Omega], \quad \text{Corollary 7.2.3} \\ &= [\Omega|_{Top^+} + \Omega|_{Top^-}, \Omega|_{Top^+} + \Omega|_{Top^-}] \\ &= [\Omega|_{Top^+}, \Omega|_{Top^+}] + [\Omega|_{Top^-}, \Omega|_{Top^-}] + 2[\Omega|_{Top^+}, \Omega|_{Top^-}]. \end{aligned}$$

Case 2. R is not a field. We have

$$\begin{aligned} [\Omega|_{X(\mathrm{min})}, \Omega|_{X(\mathrm{min})}] &= o(\mathrm{m}V/\mathrm{min}V), \quad \text{Corollary 7.2.3} \\ &= o(\mathrm{m}V) - o(\mathrm{min}V) + 1, \quad \text{Lemma 2.6.2} \\ &= (o(V) - 1) - 2 + 1, \quad \text{Lemma 2.6.2} \\ &= o(V) - 2 \\ &= [\Omega, \Omega] - 2, \quad \text{Corollary 7.2.3} \\ &= [\Omega|_{X(\mathrm{min})}, \Omega|_{X(\mathrm{min})}] + [\Omega|_{Top}, \Omega|_{Top}] + 2[\Omega|_{X(\mathrm{min})}, \Omega|_{Top}], \end{aligned}$$

whence

$$[\Omega|_{Top}, \Omega|_{Top}] + 2[\Omega|_{X(\mathrm{min})}, \Omega|_{Top}] = 2,$$

as required. □

Denote by $\mathrm{PSp} = \mathrm{Sp}/Z(\mathrm{Sp}) = \mathrm{Sp}/\{1, \iota\}$ the projective symplectic group.

7.2.5 Proposition Suppose that $q > 3$. Then Top^- and Top^+ afford faithful representations of Sp and PSp, respectively.

Proof: We divide the proof into two cases.

Case 1. R is a field. Since ι does not act trivially on Top^- and Top^+ does not afford the trivial representation, the result follows from Theorem 2.2.8.

Case 2. R is not a field. The result follows from Theorem 2.2.8, as above, if we can show that Sp(min) does not act trivially on $Top^{\pm}$. For this purpose, fix a non-zero element r in min and define $g \in \mathrm{Sp}(\mathrm{min}) \cap \mathrm{Sp}_{M,N}$ by $v_1 \mapsto (1+r)v_1$, $u_1 \mapsto (1+r)^{-1}u_1$, and all other basis vectors u_i, v_j remain fixed. Set $X = X_M$. Since $\det g|_N = 1 + r$ is a square, (5.8) gives $W(g)\frac{1\pm\iota}{2}(1 - h(\mathrm{min}))e_{v_1} = \frac{1\pm\iota}{2}(1 - h(\mathrm{min}))e_{(1+r)v_1}$. Now use (6.8) applied to $I = \mathrm{min}$, to verify that $Top^{\pm} \ni \frac{1\pm\iota}{2}(1 - h(\mathrm{min}))e_{v_1} \neq \frac{1\pm\iota}{2}(1 - h(\mathrm{min}))e_{(1+r)v_1}$. □

7.3 Weil representations associated to different characters

Given primitive linear characters $\lambda, \tau : R^+ \to F^*$, what is the relationship between W_λ and W_τ? An initial approach to this question was taken in Proposition 5.7.2, based on the actual appearance of W_λ. A more satisfactory answer is given in Theorem 7.3.1 below, whose proof is independent of Theorem 5.6.1.

In view of (2.15), (2.16) and (2.17), conjugation by $g \in \mathrm{GSp}$ restricts to an inner automorphism of Sp if $k(g) \in R^*$ is a square. As shown below, the converse is also true and lies at the heart of the problem.

7.3.1 Theorem GSp acts transitively on the set of Weil characters. Moreover, if $X = X_M$ and $g \in \mathrm{Sp}$, $k \in R^*$ then

$$W_\lambda^{B_k}(g) = W_{\lambda[k]}(g), \tag{7.6}$$

$$W_{\lambda[k^2]}(g) = W_\lambda(g_k)W_\lambda(g)W_\lambda(g_k)^{-1} \tag{7.7}$$

and

$$W_\lambda \simeq W_{\lambda[k]} \Leftrightarrow \lambda \sim \lambda[k]. \tag{7.8}$$

In words, W_λ and $W_{\lambda[k]}$ are similar if and only if k is a square. Thus conjugation by $g \in \mathrm{GSp}$ restricts to an inner automorphism of Sp if and only of $k(g) \in R^*$ is a square.

Furthermore, the relations (7.6) and (7.7) hold in all FSp-submodules Z of X. The same is true for (7.8) provided $Z = X^{\pm}$ when R is a field and $Z = Y(I), Y(I)^{\pm}$ when R not a field and (I, J) is any non-trivial A-pair.

Proof: In view of (2.15) and Corollary 4.2.2, we have

$$\eta_\lambda^{B_k} = \eta_{\lambda[k]},$$

whence

$$S_\lambda^{B_k} \simeq S_{\lambda(k)}.$$

Set $X = X_M$. Given $h \in H$, write $h = (r, u + w)$ for unique $r \in R$ and $u \in M$, $w \in N$. Then

$${}^{B_k}h = (kr, ku + w),$$

whence (5.9), (5.10) and (5.11) give

$$S_\lambda^{B_k}(0, w)e_v = e_{v+w}, \tag{7.9}$$

$$S_\lambda^{B_k}(0, u)e_v = \lambda(2k\langle u, v\rangle)e_v, \tag{7.10}$$

$$S_\lambda^{B_k}(r, 0)e_v = \lambda(kr)e_v \tag{7.11}$$

for all $v \in N$. Comparing (5.9), (5.10), (5.11) with (7.9), (7.10), (7.11) we conclude that

$$S_\lambda^{B_k}(h) = S_{\lambda(k)}(h) \tag{7.12}$$

for all $h \in H$. In view of (7.12) and the absolute irreducibility of $S_{\lambda[k]}$ we deduce that $W_\lambda^{B_k}$ must be equal to:

- The Weil representation $W_{\lambda[k]}$ associated to $\lambda[k]$, if Sp is perfect.
- Some Weil representation associated to $\lambda[k]$, if Sp is imperfect. Note however that

$$W_\lambda^{B_k}(\rho_{1,u_1}) = W_\lambda({}^{B_k}\rho_{1,u_1}) = W_\lambda(\rho_{k,u_1}),$$

whence $\Omega_\lambda^{B_k}(\rho_{1,u_1}) = \sum(\lambda[k])$, due to (5.6). Lemma 5.8.1 ensures that $W_\lambda^{B_k} = W_{\lambda[k]}$, as claimed.

Applying (2.15) and (2.17) to (7.6) we obtain (7.7). Since the processes $g \mapsto W_\lambda^{B_k}(g)$ and $g \mapsto W_\lambda(g)|_Z$ commute, (7.6) and (7.7) hold in all FSp-submodules Z of X.

In light of (2.16), (2.17) and (7.7), conjugation by $g \in \mathrm{GSp}$ restricts to an inner automorphism of Sp and $W_\lambda \simeq W_{\lambda[k(g)]}$, provided $k(g)$ is a square.

Assume henceforth that k is not a square. Two cases arise:

Case 1. R is not a field. Recall that $\mathbf{m}$ denotes a fixed generator of the minimal ideal min of R. Let $g = \rho_{\mathbf{m},u_1}$. In view of Lemma 3.2.6 and (5.6) we have

$$\Omega_{\lambda(k)}(g) = |R|^{n-1}\sum(\lambda[k\mathbf{m}]) = \left(\frac{k}{R}\right)|R|^{n-1}\sum(\lambda[\mathbf{m}]) = \left(\frac{k}{R}\right)\Omega_\lambda(g). \tag{7.13}$$

This proves that $\Omega_{\lambda[k]} \neq \Omega_\lambda$. Furthermore, suppose that (I,J) is a non-trivial A-pair. Then $J \subseteq \mathfrak{m}$, whence $\mathrm{min} \subseteq K$. Thus

$$g \in \mathrm{Sp}(\mathrm{min}) \subseteq \mathrm{Sp}(K),$$

whereby g acts trivially on $X(I)$ in virtue of Theorem 7.1.1. It follows that

$$\Omega_{Y(I),\lambda}(g) = \Omega_\lambda(g) - \Omega_{X(I),\lambda}(g) = \Omega_\lambda(g) - \dim X(I). \tag{7.14}$$

Combining (7.13) and (7.14) we deduce that $\Omega_{Y(I),\lambda[k]} \neq \Omega_{Y(I),\lambda}$.

In light of Lemmas 6.4.2 and 6.4.3 we have

$$\Omega_{Y(I),\lambda}(\iota g) = \Omega_\lambda(\iota g) - \Omega_{X(I),\lambda}(\iota g) = \mu(-1)^n - \mu(-1)^n = 0. \tag{7.15}$$

Thus Lemma 6.4.1 gives

$$\Omega_{Y(I)^\pm,\lambda}(g) = \Omega_{Y(I),\lambda}(g)/2,$$

whence $\Omega_{Y(I)^\pm,\lambda[k]} \neq \Omega_{Y(I)^\pm,\lambda}$, in virtue of (7.13) and (7.14).

Case 2. $R = F_q$. Let $g = \rho_{1,u_1}$. Applying the above reasoning we obtain

$$\Omega_{\lambda[k]}(g) = \left(\frac{k}{q}\right)\Omega_\lambda(g), \tag{7.16}$$

which proves that $\Omega_{\lambda[k]} \neq \Omega_\lambda$. Furthermore,

$$\Omega_{X^\pm,\lambda}(g) = (\Omega_\lambda(g) \pm \mu(-1)^n)/2 \tag{7.17}$$

due to Lemmas 6.4.1 and 6.4.2. It follows from (7.17) and (7.16) that $\Omega_{X^\pm,\lambda[k]} \neq \Omega_{X^\pm,\lambda}$, as claimed.

We conclude that conjugation by $g \in \mathrm{GSp}$ does not restrict to an inner automorphism of Sp if $k(g)$ is not a square.

7.4 Character fields

We have accumulated enough machinery to describe the character fields of the Weil representations.

7.4.1 Theorem $\mathrm{Gal}(F/\mathbf{Q})$ acts transitively on the set of Weil characters. In fact,

$$^{\sigma(k)}\Omega_\lambda = \Omega_{\lambda[k]}$$

for all $k \in (\mathbf{Z}/p^e\mathbf{Z})^*$. Furthermore, let $X = X_M$ and consider the Weil representations as matrix representations relative to the F-basis $(e_v)_{v\in N}$ of X. Then

$$^{\sigma(k)}W_\lambda = W_{\lambda[k]} \tag{7.18}$$

and

$$^{\sigma(k^2)}W_\lambda(g) = W_\lambda(g_k)W_\lambda(g)W_\lambda(g_k)^{-1} \tag{7.19}$$

for all $g \in \mathrm{Sp}$.

If (I, J) is any A-pair then (7.18) and (7.19) hold on the FSp-submodules $X(I)$, $X(I)^\pm$, $Y(I)^\pm$ and $Y(I)$ of X, relative to their bases $\mathcal{B}(I)$, $\mathcal{B}^\pm(I)$, $\mathcal{C}^\pm(I)$ and $\mathcal{C}^+(I) \cup \mathcal{C}^-(I)$. Thus, if $Z = X$, $X^\pm$, $Y(I)$ or $Y(I)^\pm$ then

$$\mathbf{Q}(\Omega_{\lambda,Z}) = \mathbf{Q}\left(\sqrt{(\tfrac{-1}{q})q}\right). \tag{7.20}$$

Proof: (Eq. 7.18) can be read off from Theorem 5.6.1. Alternatively, Corollary 4.2.4 gives

$$^{\sigma(k)}\eta_\lambda = \eta_{\lambda[k]}.$$

Reasoning as in the proof of Theorem 7.3.1 we discover that actually

$$^{\sigma(k)}S_\lambda = S_{\lambda[k]}, \tag{7.21}$$

relative to the basis $(e_v)_{v\in N}$ of $X = X_M$. Reasoning again as in the proof of Theorem 7.3.1 we see that (7.21) implies that $^{\sigma(k)}W_\lambda$ is equal to:

- The Weil representation $W_{\lambda[k]}$ associated to $\lambda[k]$, if Sp is perfect.
- Some Weil representation associated to $\lambda[k]$, if Sp is imperfect. Note however that

$$^{\sigma(k)}\Omega_\lambda(\rho_{1,u_1}) = {}^{\sigma(k)}(\Omega_\lambda(\rho_{1,u_1})) = {}^{\sigma(k)}(\sum(\lambda)) = \sum(\lambda[k]),$$

hence Lemma 5.8.1 ensures that $^{\sigma(k)}W_\lambda = W_{\lambda[k]}$.

(Eq. 7.19) follows from (7.18), (7.6) and (7.7). Since the matrix of change of basis from $(e_v)_{v\in N}$ to $\mathcal{B}(I)^+\cup\mathcal{B}(I)^-\cup\mathcal{C}(I)^+\cup\mathcal{C}(I)^-$ has rational entries (7.18) and (7.19) also hold on $X(I)$, $Y(I)$, $X(I)^\pm$ and $Y(I)^\pm$.

The last assertion follows from the above, Theorem 7.3.1 and Lemma 2.2.1(f). □

7.5 Schur indices

The Weil representations afforded by $Top^\pm$ will be thought of as matrix representations relative the bases (6.14).

7.5.1 Theorem (a) Top^+ can be realized over its character field $\mathbf{Q}\left(\sqrt{(\frac{-1}{q})q}\right)$.

(b) Top^- can be realized over its character field $\mathbf{Q}\left(\sqrt{(\frac{-1}{q})q}\right)$ if and only if $\mathbf{Q}\left(\sqrt{(\frac{-1}{q})q}\right)$ is not a real field, that is, if $q \equiv 3 \mod 4$. The Schur index of Top^- over $\mathbf{Q}$ is precisely two if $q \equiv 1 \mod 4$.

Proof: We shall implicitly use the results proven in Theorems 7.3.1 and 7.4.1. The translation of Proposition 3.4.6 into our setting reads as follows:

- $T = W_{Top^\pm}$;

- $\mathbf{F} = F$;
- $\mathbf{K} = \begin{cases} \mathbf{Q} & \text{if } q \text{ is a square,} \\ \mathbf{Q}\left(\sqrt{(\frac{-1}{q})q}\right) & \text{otherwise;} \end{cases}$
- $\sigma = \begin{cases} \sigma_x & \text{if } q \text{ is a square,} \\ \sigma_{x^2} & \text{otherwise,} \end{cases}$ where x is a generator of $(\mathbf{Z}/p^e\mathbf{Z})^*$;

Let y be any of the two elements of R^* satisfying

$$\begin{cases} y^2 = x & \text{if } q \text{ is a square,} \\ y^2 = x^2 & \text{otherwise,} \end{cases}$$

Such y exists due to Lemma 2.2.1;

- $L = W_{Top^\pm}(g_y)$;
- $r = \begin{cases} p^{e-1}(p-1) & \text{if } q \text{ is a square,} \\ p^{e-1}(p-1)/2 & \text{otherwise} \end{cases}$

Thus r = order of $\sigma = \frac{\text{order of } y}{2}$. In view of Lemma 6.2.1

$$^{\sigma^{r-1}}L \ldots {}^{\sigma}LL = L^r = W_{Top^\pm}(g_{y^r}) = W_{Top^\pm}(\iota) = \pm 1_{Top^\pm},$$

whence

- $a = \pm 1$.

In view of Proposition 3.4.6, (a) is proven.

(b) If $q \equiv 3 \mod 4$ then $p \equiv 3 \mod 4$ and $[\mathbf{F} : \mathbf{K}] = p^{e-1}(p-1)/2$ is odd. Therefore $N_{\mathbf{F}/\mathbf{K}}(-1) = (-1)^{[\mathbf{F}:\mathbf{K}]} = -1$, whence Top^- can be realized over $\mathbf{K}$.

Suppose henceforth that $q \equiv 1 \mod 4$. Then $[\mathbf{F} : \mathbf{K}]$ is always even and $\mathbf{K} = \mathbf{Q}\left(\sqrt{(\frac{-1}{q})q}\right)$ is always a real field. Pairing each $\tau \in \mathrm{Gal}(\mathbf{F}/\mathbf{K})$ with its complex conjugate we see that $N_{\mathbf{F}/\mathbf{K}}(x)$ is always non-negative. Thus $N_{\mathbf{F}/\mathbf{K}}(x) = -1$ is unsolvable and the Schur index cannot be one. The fact that it is precisely two follows from the Brauer-Speiser theorem [Fei70].

7.6 The case of a principal ring

Assume here that R is an irreducible ring. The case $R = (0)$ will be extraordinarily allowed, in which case we shall assume that H, Sp and the terms Schrödinger and Weil representations have the trivial meaning.

Fix a primitive linear character λ of R^+ and an A-pair (I, J). Let $K = (I : J)$ and adopt the notation (2.27) for the ideal K, unless otherwise stated.

The results described in this section generalize and extend work that was originally started in collaboration with Gerald Cliff and David A. McNeilly.

7.6.1 Proposition Let (I, J) be an A-pair and let $K = (I : J)$. Suppose that $J/I = Rt + I$ is principal and let $G = (J^2, JV) \subseteq H$. Then

$$G/D(I) \ni (t^2 r, tv)(0, IV) \to (\overline{r}, \overline{v}) \in \overline{H} \tag{7.22}$$

is a group isomorphism. If $\overline{h}$ denotes the image of $h \in G$ under (7.22) then

$$\overline{{}^g h} = {}^{\overline{g}}\overline{h} \tag{7.23}$$

for all $h \in G$ and $g \in \mathrm{Sp}$.

The representation $\overline{S}$ of $\overline{H}$ afforded by $X(I)$ via (7.22) is the Schrödinger representation associated to the character $\overline{\lambda}$ of $\overline{R}$, defined by

$$\overline{\lambda}(\overline{r}) = \lambda(t^2 r). \tag{7.24}$$

Proof: We first observe that the set-up makes sense. Indeed, since (I, J) is an A-pair and $J/I = Rt + I$ the ideal $J^2 = (t^2)$ is principal. But in view of (3.14) and Lemma 3.2.7 J^2 is the annihilator of K, whence Lemma 3.2.8 ensures that R/K does admit the primitive linear character $\overline{\lambda}$.

Now the first two assertions follow from the very definition of the objects involved. Proposition 6.1.2 shows that $X(I)$ is an absolutely irreducible $F(G/D(I))$, and hence $F(\overline{H})$-module. By definition

$$\overline{S}(\overline{h}) = S(h)|_{X(I)}, \quad h \in G. \tag{7.25}$$

In particular, if $h = (t^2 r, 0)$ then (7.25) reads

$$\overline{S}(\overline{r}, 0) = S(t^2 r, 0)_{X(I)} = \lambda(t^2 r) 1_{X(I)} = \overline{\lambda}(\overline{r}) 1_{X(I)}.$$

Theorem 4.1.4 guarantees that $\overline{S}$ is the Schrödinger representation associated to $\overline{\lambda}$. □

7.6.2 Theorem Let (I, J) be any A-pair. The restriction to $\mathrm{Sp}(K)$ of the Weil representation $W_{\lambda, X(I)}$ of Sp afforded by $X(I)$ is trivial. The corresponding representation $\overline{W}$ of $\overline{\mathrm{Sp}}$ is a Weil representation if and only if J/I is principal, in which case the associated character is (7.24).

Proof: Since $K = (I : J)$, Theorem 7.1.1 asserts that $W_{\lambda, X(I)}$ is trivial when restricted to $\mathrm{Sp}(K)$.

Suppose first that $J/I = Rt + I$ is principal. The very definitions of $\overline{S}$ and $\overline{W}$, and the compatibility condition (7.23) show that the equation

$$W(g)|_{X(I)} S(h)|_{X(I)} W(g)^{-1}|_{X(I)} = S({}^g h)|_{X(I)}, \quad g \in \mathrm{Sp}, h \in G$$

can be written as

$$\overline{W}(\overline{g}) \overline{S}(\overline{h}) \overline{W}(\overline{g})^{-1} = \overline{S}({}^{\overline{g}} \overline{h}), \quad \overline{g} \in \overline{\mathrm{Sp}}, \overline{h} \in \overline{H}. \tag{7.26}$$

Since $\overline{S}$ is the Schrödinger representation of $\overline{H}$ associated to $\overline{\lambda}$, (7.26) says that $\overline{W}$ is a Weil representation of $\overline{\mathrm{Sp}}$ associated to $\overline{\lambda}$. Two cases arise:

$\overline{\mathrm{Sp}}$ is perfect. There is nothing to be done.

$\overline{\mathrm{Sp}}$ is imperfect. Then $n = 1$ and $q = 3$. We need to verify that the character $\overline{\Omega}$ of $\overline{W}$ satisfies the condition of Lemma 5.8.1. That is,

$$\Omega_{\lambda, X(I)}(\rho_{1, u_1}) = \overline{\Omega}(\rho_{\overline{1}, \overline{u_1}}) = \sum_{\overline{r} \in \overline{R}} \overline{\lambda}(\overline{r}^2) \tag{7.27}$$

To compute $\Omega_{\lambda, X(I)}(\rho_{1, u_1})$ we use the basis (6.11) of $X(I)$. Note that $N = Rv_1$. Set $g = \rho_{1, u_1} \in \mathrm{Sp}^M$ and $\mathcal{T} = \mathcal{T}(Jv_1/Iv_1) = \mathcal{T}(J/I)$. Then (5.4) gives

$$W_\lambda(g) \widehat{e_v} = \frac{1}{|I|} \sum_{w \in Iv_1} \lambda(\langle g(v+w), v+w \rangle) e_{v+w} = \lambda(\langle gv, v \rangle) \widehat{e_v} \quad v \in \mathcal{T}$$

since $\langle v_0, w_0 \rangle = 0$ for all $v_0 \in Jv_1$ and $w_0 \in Iv_1$. Thus

$$\Omega_{\lambda, X(I)}(g) = \sum_{v \in \mathcal{T}} \lambda(\langle gv, v \rangle) = \sum_{r \in \mathcal{T}} \lambda(\langle grv_1, rv_1 \rangle) = \sum_{r \in \mathcal{T}} \lambda(r^2). \tag{7.28}$$

On the other hand, in view of the bijection

$$R/K \ni r + K \leftrightarrow rt + I \in J/I \tag{7.29}$$

we can write

$$\sum_{r \in \mathcal{T}} \lambda(r^2) = \sum_{rt + I \in J/I} \lambda(t^2 r^2) = \sum_{\overline{r} \in \overline{R}} \lambda(t^2 r^2) = \sum_{\overline{r} \in \overline{R}} \overline{\lambda}(\overline{r}^2) \tag{7.30}$$

In light of (7.28) and (7.30), (Eq. 7.27) is established.

Suppose now, conversely, that $X(I)$ affords a Weil representation of $\overline{\mathrm{Sp}}$. First of all observe that

$$|J/I|^n = \deg X(I) = |R/K|^n \tag{7.31}$$

due to Proposition 6.1.2 and Theorem 4.1.4.

In view of Corollary 7.2.2 $X(I)$ affords a faithful representation of $\overline{\mathrm{Sp}}$. Thus, if this is a Weil representation it must be associated to a primitive linear character of $\overline{R}$ (one can associate Weil representations to any linear character; only if the character is primitive the resulting representation will be faithful). Therefore K is an irreducible ideal.

Now $K = \cap_{x \in J}(I : (x))$, hence

$$K = (I : (t)) \tag{7.32}$$

for some $t \in J$ due to the irreducibility of K. It follows from (7.32) that (7.29) is an injection, and hence a bijection in light of (7.31). We conlcude that J/I is principal, as claimed. □

7.6.3 Note On the day this thesis was submitted a proof of the following result was nearly finished: $X(I)$ affords a tensor product of Weil representations of $\overline{\mathrm{Sp}}$ if and only if J^2 is principal.

7.6.4 Theorem IF R is principal then X decomposes as the sum of $l+1$ absolutely irreducible FSp-modules non-equivalent to one another. There are $\lfloor l/2 \rfloor$ of them contained in each of $X^{\pm}$, with degrees $q^{n(l-2(i+1))}(q^{2n}-1)/2$, $0 \leq i < \lfloor l/2 \rfloor$, plus the one dimensional trivial module $X(\pi^{l/2})$ if l is even and the q^{2n}-dimensional module $X(\pi^{(l+1)/2})$ affording the Weil representation of $\mathrm{Sp}_{2n}(q)$ and having absolutely irreducible components $X(\pi^{(l+1)/2})^{\pm}$ if l is odd.

Proof: By induction on l. If $l=0$ then $R=(0)$, $\mathrm{Sp}=\{1\}$ and X is the one-dimensional trivial module. The field case was already treated in Theorem 7.2.4. Suppose that $l>1$ and the result is true for all R with nilpotency degree less than l. By Theorem 7.6.2 and inductive hypothesis, $X(\mathrm{min}) = X(\pi^{l-1})$ breaks up into the sum of $l-1$ absolutely irreducible FSp-modules of the desired degrees. Since $X = Top^{+} \oplus Top^{-} \oplus X(\mathrm{min})$, Corollary 7.2.3 and Lemma 2.6.1 guarantee that $Top^{\pm}$ and the $l-1$ components of $X(\mathrm{min})$ are all absolutely irreducible and non-equivalent to one another. The degrees of $Top^{\pm}$ are given in Lemma 6.1.3. □

The next result gives the entire decomposition of X, without recurring to Theorem 7.6.2.

7.6.5 Theorem Suppose that R is principal and let $\mathcal{D}^{\pm} = \mathcal{D}^{\pm}(\mathcal{C})$, where $\mathcal{C}$ is the strictly ascending chain of A-pairs

$$(0,R) = (\mathfrak{m}^{l},\mathfrak{m}^{0}) < (\mathrm{min},\mathfrak{m}) = (\mathfrak{m}^{l-1},\mathfrak{m}^{1}) < \ldots < (\mathfrak{m}^{\lceil l/2 \rceil},\mathfrak{m}^{\lfloor l/2 \rfloor}).$$

Then $\mathcal{D}^{\pm}$ give *the* decomposition of X into $l+1$ absolutely irreducible non-zero FSp-components, non-isomorphic to one another.

Proof: According to (6.18) the number of non-zero components of $\mathcal{D}^{\pm}$ is always equal to $l+1$, regardless of the parity of l. The fact that they are absolutely irreducible and non-isomorphic follows from Corollary 7.2.3 and Lemma 2.6.1. □

7.7 The case of a homogeneous ring

Assume here that R is a homogeneous ring and fix an ideal I which is its own annihilator. We prove that then $Top^{\pm}$ and Top afford monomial characters of Sp.

Set $L = L_{I,I} = IV$ and $X = X_L$. Then $P = P_L$ is equal to W, as shown in Lemma 6.1.3; there is no need to deal with projective representations.

Given $v \in V$, denote by $\mathrm{Sp}(I, v)$ the subgroup of Sp consisting of all g satisfying $gv \equiv v \mod IV$. In view of (4.10) the map $\delta_v : \mathrm{Sp}(I, v) \to F^*$

$$g \mapsto \lambda(\langle gv, v\rangle)$$

is a linear character. Observe that

$$\mathrm{Sp}(I, v) \times \langle \iota \rangle = \{g \in \mathrm{Sp} \mid gv \equiv \pm v \mod IV\} \tag{7.33}$$

and denote by $\delta_v^{\pm}$ the extension of δ_v to $\mathrm{Sp}(I, v) \times \langle \iota \rangle$ defined by $\delta_v^{\pm}(\iota) = \pm 1$.

The next result was originally proved by Gerald Cliff for a principal ring R.

7.7.1 Theorem Ω_{Top} and $\Omega_{Top^{\pm}}$ are monomial characters. In fact,

$$\Omega_{Top^{\pm}} = \mathrm{ind}_{\mathrm{Sp}(I,v)\times\langle\iota\rangle}^{\mathrm{Sp}} \delta_v^{\pm} \tag{7.34}$$

and $\Omega_{Top} = \mathrm{ind}_{\mathrm{Sp}(I,v)}^{\mathrm{Sp}} \delta_v$ for any $v \in \mathcal{P}$.

Proof: Let $\mathcal{T} = \mathcal{T}(V/L)$ and let $\mathcal{T}_{\mathfrak{m},I}$ be the transversal of $\mathfrak{m}V$ relative to IV contained within it. Set $\mathcal{P}_0 = \{v \in \mathcal{T} : v \notin \mathfrak{m}V\} = \mathcal{T} \setminus \mathcal{T}_{\mathfrak{m},I}$. Lemma 6.2.3 shows that $(e_v)_{v\in\mathcal{T}_{\mathfrak{m},I}}$ is a basis of $X(\mathsf{min})$. Denote temporarily by Z the F-subspace of X with basis $(e_v)_{v\in\mathcal{P}_0}$. Since Z is FSp-invariant (use (4.10) or Proposition 6.2.3) and complements $X(\mathsf{min})$ we necessarily have $Z = Top$.

Since Sp acts transitively on $\mathcal{P}_0$ (Corollary 2.2.3), (4.10) tells us that Sp permutes transitively the one-dimensional subspaces of X spanned by the basis vectors $(e_v)_{v\in\mathcal{P}_0}$. Moreover, given a fixed vector $v \in \mathcal{P}_0$, we recognize the stabilizer of Fe_v in Sp as $\mathrm{Sp}(I, v)$, affording the character δ_v. Thus, $\Omega_{Top} = \mathrm{ind}_{\mathrm{Sp}(I,v)}^{\mathrm{Sp}} \delta_v$, as claimed.

Write $f_v^{\pm} = e_v \pm e_{-v}$, $v \in \mathcal{P}$, and observe the relations:

$$W(\iota) f_v^{\pm} = f_{-v}^{\pm} = \pm f_v^{\pm},$$

$$W(g) f_v^{\pm} = \lambda(\langle gv, v^{\wedge} \rangle) f_{v'}^{\pm},$$

in the notation of (4.10). Reasoning as above, and taking into account (7.33), we see that $\Omega_{Top^{\pm}} = \mathrm{ind}_{\mathrm{Sp}(I,v)\times\langle\iota\rangle}^{\mathrm{Sp}} \delta_v^{\pm}$ for any $v \in \mathcal{P}_0$. □

Examples

Example 1 Let $R = F_q[s,t]$, subject to the relations $s^2 = t^2 = 0$. Then $X(\mathrm{min})$ affords the permutation representation of $\mathrm{Sp}_{2n}(q) \simeq \mathrm{Sp}_{2n}(R)/\mathrm{Sp}(\mathfrak{m})$ arising from its natural action on a symplectic F_q-space of dimension $2n$.

Proof: R is local since the maximal ideal $\mathfrak{m} = (s,t)$ is nilpotent. The nilpotency degree of $\mathfrak{m}$ is equal to $l = 3$, while $\mathrm{min} = \mathfrak{m}^2 = (st)$ is the unique minimal ideal of R. The cardinality of R is q^4.

Proposition 6.1.2 gives $\dim X(\mathrm{min}) = |\mathfrak{m}/\mathrm{min}|^n = q^{2n}$, as required. To compute with $X(\mathrm{min})$ we shall let $I = (s)$, so that $\mathrm{Ann}(I) = I$, and take $X = X_{IV}$.

Choose $\mathcal{T} = \mathcal{T}(V/IV)$ and let $\mathcal{T}_0$ be the transversal $\mathcal{T}_0$ of $\mathfrak{m}V$ relative to IV contained within it. Then Lemma 6.2.3 shows that $(e_v)_{v\in\mathcal{T}_0}$ is a basis of $X(\mathrm{min})$. To be specific, let $W = F_q u_1 \oplus \ldots \oplus F_q u_n \oplus F_q v_1 \oplus \ldots \oplus F_q v_n$ and observe that $V = W \oplus sW \oplus tW \oplus stW = (W \oplus tW) \oplus (IV)$. We can thus take $\mathcal{T} = \mathcal{T}(V/IV) = W \oplus tW$ and $\mathcal{T}_0 = tW$. Observe that $(W, \langle,\rangle|_{W\times W})$ is a $2n$ dimensional symplectic space over F_q; another such symplectic space is $(tW, \langle,\rangle_t)$, where $\langle tx, ty\rangle_t = \langle x, y\rangle$ for all $x, y \in W$. The symplectic group corresponding to each of them is precisely the subgroup of $\mathrm{Sp}_{2n}(R)$ preserving W. There is no danger of confusion if we denote this subgroup by $\mathrm{Sp}_{2n}(q)$.

According to this definition, we have $\mathrm{Sp}_{2n}(R) = \mathrm{Sp}(\mathfrak{m}) \rtimes \mathrm{Sp}_{2n}(q)$. Since $(\mathrm{min} : \mathfrak{m}) = \mathfrak{m}$, Theorem 7.1.1 tells us that $\mathrm{Sp}(\mathfrak{m})$ acts trivially on $X(\mathrm{min})$. We proceed to compute the corresponding representation of $\mathrm{Sp}_{2n}(q)$ afforded by $X(\mathrm{min})$. Given $v \in \mathcal{T}_0$ and $g \in \mathrm{Sp}$, Lemma 6.1.4 and (4.10) tell us that $W(g)e_v = \lambda(\langle gv, v'\rangle)e_{v'}$, where $gv \equiv v' \mod IV$ for a unique $v' \in \mathcal{T}_0$. Since v, gv and v' belong to tV and $(t)^2 = (0)$, we have $\lambda(\langle gv, v'\rangle) = 1$.

Since $\mathrm{Sp}_{2n}(q)$ preserves $\mathcal{T}_0$, $v' = gv$. We have thus proven that

$$W(g)e_v = e_{gv}$$

for each $g \in \mathrm{Sp}_{2n}(q)$ and each $v \in ({}^tW, \langle , \rangle_t)$, as claimed. □

Example 1 shows that:

(a) Strong results such as Theorem 7.6.2 cannot possibly hold for a general special ring R.

(b) Strong statements such as (7.8) might fail miserably on $X(I)$, let alone on an arbitrary FSp-submodule Z of X. This pathology is essentially impossible when R is principal. Indeed, in this case, $W_{\lambda,Z} \simeq W_{\lambda[k],Z}$ for a non-square $k \in R^*$ if and only if l is even and $Z = X(\pi^{\lambda/2})$ affords the trivial representation.

(c) There is no hope, in general, that F is sufficiently large to ensure that all the irreducible Weil components are absolutely irreducible. Indeed, even if $n = 1$, the permutation $\mathbf{C}\mathrm{Sp}_{2n}(q)$-module $\widehat{V}$ has components whose character values lie outside F, except when $q = 3$ ([Tie97] § 3, [Dor71] § 38). This pathology cannot occur when R is principal.

Example 2 Let (I, J) be a B-pair in an irreducible ring R (the existence of such pair is ensured by Proposition 3.2.9) and let $d = \dim_{F_q} J/I$. One can use the results of section 7.6 to show that, depending on the nature of d, $X(I)$ affords the following representation of $Sp_{2n}(q)$:

$$d = \begin{cases} 0 & \Rightarrow \text{trivial representation,} \\ 1 & \Rightarrow \text{Weil representation,} \\ \geq 2 & \Rightarrow \text{tensor product of } d \text{ Weil representations.} \end{cases}$$

Example 1 is a particular instance of this phenomenon.

Topics for further investigation

There is an explicit formula to realize the Weil representations of $\mathrm{Sp}_{2n}(q)$ afforded by $X^{\pm}$, provided $m_{\mathbf{Q}}(\Omega_{X^{\pm}}) = 1$ [Sze98]. It is natural then to pose

Problem 1 Suppose that $m_{\mathbf{Q}}(\Omega_{X^{\pm}}) = 1$. When and how are $W_{X^{\pm}}$ realizable over the ring of integers of $\mathbf{Q}(\Omega_{X^{\pm}})$? What can be said about the corresponding lattice?

For instance, if q is square, it is definitely possible to conjugate W_{X^+} into a matrix representation with coefficients in $\mathbf{Z}$. We even wrote an algorithm that given an input I consisting of a finite set of rational $d \times d$ invertible matrices, produces as output a conjugate set O of integral matrices, provided I generates a finite group. There seems to be no way, yet, to write down a closed formula for the matrix that performs the conjugation.

Work in the general case of an irreducible ring can be continued with

Problem 2 Describe $X(\mathsf{min})$ in as much detail as possible.

Nice as it might be, Theorem 7.7.1 is false, in general, if R is not homogeneous. It is reasonable then to pose

Problem 3 Find necessary and sufficient conditions for $Top^{\pm}$ to afford monomial characters. Find subgroups $G^{\pm}$ and $G^{\pm}$-modules $Z^{\pm}$ such that $Top^{\pm} = \mathrm{ind}_{G^{\pm}}^{\mathsf{Sp}} Z^{\pm}$.

David A. McNeilly has made progress in regards to Problem 3.

Lemma 4.2.5 invites us to write down W relative to different models of X. This might allow us to see W from different perspectives than that of Theorem 5.6.1, and discover further properties, as in the case when R is homogeneous. This prompts us to pose

Problem 4 Find explicit H-isomorphisms between the different models of X given

in Lemma 4.2.5. Then use Theorem 5.6.1 and the H-isomorphism $X \simeq X_M$ to write down W relative to X.

Bibliography

[AM69] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Massachusetts, 1969.

[BRW61] B. Bolt, T.G. Room, and G.E. Wall, *On the Clifford collineation, transform, and similarity groups. I*, J. Austral. Math. Soc. **2** (1961), 60–79.

[CMS] G. Cliff, D.A. McNeilly, and F. Szechtman, *Weil representations of symplectic groups over rings*, Preprint.

[Die48] J. Dieudonné, *Sur les groupes classiques*, Hermann, Paris, 1948.

[Dor71] L. Dornhoff, *Group representation theory*, Marcel Dekker, New York, 1971.

[Fei70] B. Fein, *A note on the Brauer-Speiser theorem*, Proc. Amer. Math. Soc. **25** (1970), 620–621.

[Ger77] P. Gerardin, *Weil representations associated to finite fields*, J. Algebra **46** (1977), 54–101.

[Gow89] R. Gow, *Even unimodular lattices associated with the Weil representation of the finite symplectic group*, J. Algebra **122** (1989), 510–519.

[Gro90] B.H. Gross, *Group representations and lattices*, J. Amer. Math. Soc **3** (1990), 929–960.

[Hil95] G. Hill, *Regular elements and regular characters of* $\mathrm{GL}_n(\mathcal{O})$, J. Algebra **174** (1995), 610–635.

[HO89] A.J. Hahn and O.T. O'Meara, *The classical groups and K-theory*, Springer-Verlag, Berlin, 1989.

[How73] R.E. Howe, *On the characters of Weil's representations*, Trans. Amer. Math. Soc. **95** (1973), 594–635.

[Isa73] I.M. Isaacs, *Characters of solvable and symplectic groups*, Amer. J. Math. **95** (1973), 594–635.

[Jac85] N. Jacobson, *Basic algebra*, second ed., vol. I, Freeman, New York, 1985.

[Kli63] W. Klingenberg, *Symplectic groups over local rings*, Amer. J. Math. **85** (1963), 232–240.

[Kru68] W. Krull, *Idealtheorie*, second ed., Springer-Verlag, Berlin, 1968.

[Lam53] E. Lamprecht, *Allgemeine theorie der Gaußschen summen in endlichen kommutativen ringen*, Math. Nachr. **9** (1953), 149–196.

[Lan70] Lang, *Algebraic number theory*, Addison-Wesley, Reading, 1970.

[Lee78] P. Lees, *A Steinberg representation for* $\mathrm{GL}_n(Z/p^hZ)$, Proc. London Math. Soc. (3) **37** (1978), 459–490.

[O'M78] O.T. O'Meara, *Symplectic groups*, Mathematical Surveys and Monographs, Amer. Math. Soc., Providence, 1978.

[Rib72] P. Ribenboim, *Algebraic numbers*, Wiley-Interscience, New York, 1972.

[Sei75] G.M. Seitz, *Some representations of classical groups*, J. London Math Soc. (2) **115-120** (1975), 10.

[Ser79] J.-P. Serre, *Local fields*, Springer-Verlag, New York, 1979.

[ST97] R. Scharlau and P.H. Tiep, *Symplectic groups, symplectic spreads, codes, and unimodular lattices*, J. Algebra **194** (1997), 113–156.

[Sze] F. Szechtman, *Weil representations of unitary groups*, to appear in J. of Algebra.

[Sze98] F. Szechtman, *Weil representations of the symplectic group*, J. Algebra **208** (1998), 662–686.

[Tan67] S. Tanaka, *Irreducible representations of the binary modular congruence groups mod p^λ*, J. Math. Kyoto Univ. **7-2** (1967), 123–132.

[Tie97] P.H. Tiep, *Weil representations as globally irreducible representations*, Math. Nachr **184** (1997), 313–327.

[TZ97] P.H. Tiep and A. Zalesski, *Some characterizations of the Weil representations of symplectic and unitary groups*, J. Algebra **192** (1997), 130–165.

[Wan93] Z. Wan, *Geometry of classical groups over finite fields*, Studentlitteratur, Lund, 1993.

[War72] H.N. Ward, *Representation of symplectic groups*, J. Algebra **20** (1972), 182–195.

[ZS58] O. Zariski and P. Samuel, *Commutative algebra*, D. Van Nostrand, Princeton, 1958.

Index

$\mathcal{A}$, 52
$\mathrm{Ann}(I)$, 15

$\mathcal{B}(I)$, 76
$\mathcal{B}^{\pm}(I)$, 76
B_k, 20

$\mathfrak{c}$, 6
c, 57
$\mathcal{C}^{\pm}(I)$, 77

$\mathcal{D}^{\pm}(\mathcal{C})$, 79
$\widehat{\Delta}$, 83
$D(I)$, 73
d_R, 6

$E(I)$, 73
η, 50
η_λ, 50
e_v, 55

F, 6
$\langle\ ,\ \rangle$, 8
$\langle\ ,\ \rangle_I$, 24

$\overline{g}$, 24
g_I, 24
g_k, 20
$g_{M,N}$, 16
$g^M(r)$, 17
$g^N(r)$, 17
GSp, 20

H, 48
$\overline{H}$, 24
H_I, 24
h_I, 24
$h(I)$, 75

ι, 17

$k(g)$, 20

l, 6
$L^{\perp}$, 11
L^0, 11
$\lambda[r]$, 32
$(\frac{k}{R})$, 10
$L_{I,J}$, 15

$\mathcal{M}$, 14
M, 14
$\mathfrak{m}$, 6
min, 31

$\mathbf{m}$, 33
μ, 28
$\mu(G, E)$, 26

n, 8
N, 14

$o(\Delta)$, 21

p, 6
$\mathcal{P}$, 10
P, 54
p^e, 6
P_L, 55

q, 6

R, 6
$\overline{R}$, 24
$\overline{r}$, 24
ρ_0, 50
R_I, 24
R_i, 6
r_I, 24
$\rho_{r,x}$, 9

$\mathcal{S}(V/V_0)$, 55
S, 50
S_λ, 50
$\sigma(k)$, 54
Sp, 9
$\overline{\mathrm{Sp}}$, 24
Sp_I, 24
$\mathrm{Sp}(I)$, 11
Sp_M, 14
$\sum(\lambda)$, 30

$\mathcal{T}(V/V_0)$, 55
$\mathcal{T}$, 55
$\mathbf{T}(\mathcal{C})$, 79
Top, 73

u_i, 10

V, 8
$\overline{V}$, 24
$\overline{v}$, 24
V_I, 24
v_I, 24
v_i, 10

W, 53
W_λ, 53
$W_{\lambda,Z}$, 73

X, 50
$X(I)$, 73
X_L, 55
$X^{\pm}$, 72

$Y(I)$, 73

ζ_s, 6